

# THÈSES

présentées à

LA FACULTÉ DES SCIENCES DE PARIS

pour obtenir

le . . . . . GRADE . . de DOCTEUR ES SCIENCES MATHÉMATIQUES

par Monsieur MAURIN Francis - Jean

Sujet de la 1ère Thèse . . . . . " Groupes finis et construction de tableaux orthogonaux."

Sujet de la 2è Thèse ( propositions données par la Faculté )

. . " Martingales et théorèmes de convergence."

Soutenues le 2 Mars 1970 . . . . . devant la Commission

composée de Président : DUGUE

Examineurs : BENZECRI

ARIBAUD

Invité :



# THÈSES

présentées à

LA FACULTÉ DES SCIENCES DE PARIS

pour obtenir

le ..... GRADE de DOCTEUR ES SCIENCES MATHÉMATIQUES

par Monsieur MAURIN Francis - Jean

Sujet de la 1ère Thèse ..... " Groupes finis et construction de tableaux orthogonaux."

Sujet de la 2è Thèse ( propositions données par la Faculté ) .....

" Martingales et théorèmes de convergence."

Soutenues le 2 Mars 1970 ..... devant la Commission

composée de Président : DUGUE

Examineurs : BENZECHI

ARIBAUD

Invité :

23-34T

3-14-1913

WILLIAM H. HARRISON, 23-34T, 3-14-1913

1913-1914

1914-1915



## I N T R O D U C T I O N

---

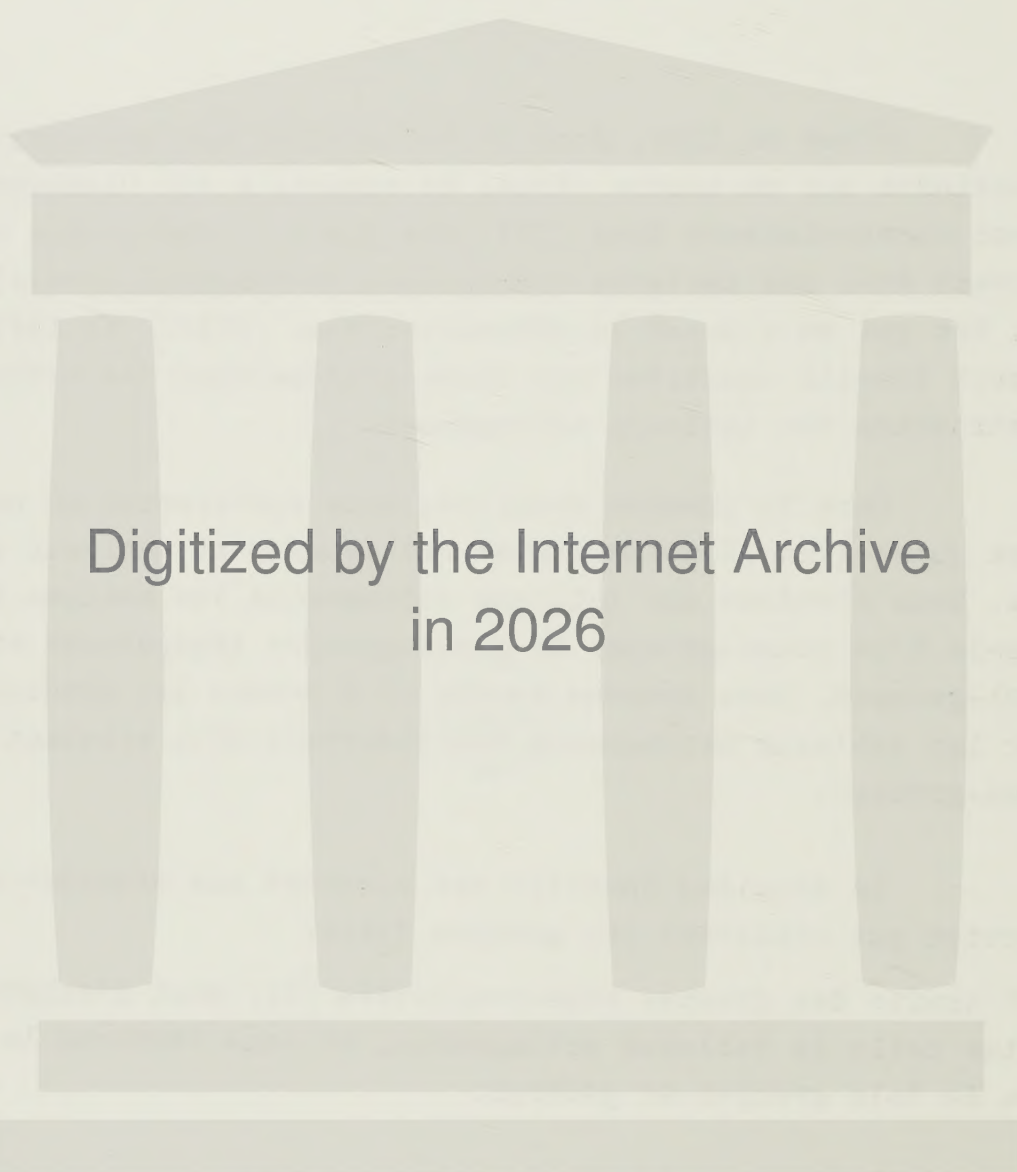
C'est en 1946, dans le but d'effectuer une analyse de la variance sur un nombre réduit de résultats que Plackett et Burman construisirent dans [XVI] des plans d'expériences qui se trouvent être des tableaux orthogonaux (orthogonal arrays). C'est C.R. Rao qui en a donné la définition dans [XVIII] en 1947. Le présent travail constitue une étude systématique des méthodes de construction des tableaux orthogonaux.

Dans le premier chapitre, nous établissons un parallèle entre quasi-groupes mutuellement orthogonaux et tableaux orthogonaux. Nous étendons aux tableaux orthogonaux les notions de transversale d'un quasi-groupe, de quasi-groupes idempotents et de sous-quasi-groupes. Nous donnons au fur et à mesure les généralisations pour les tableaux orthogonaux des théorèmes déjà existant pour les quasi-groupes.

Le deuxième chapitre est consacré aux méthodes de construction qui utilisent les groupes finis.

II.1 traite des groupes sous-transitifs [XI] dont l'existence entraîne celle de tableaux orthogonaux, et nous étudions la structure de tels groupes en général.

II.2 est consacré à l'étude détaillée des groupes sous-transitifs abéliens d'indice unité [XII] dont l'existence est liée à celle d'automorphismes propres d'un groupe abélien, et nous donnons une condition nécessaire et suffisante d'existence de tels groupes. Nous examinons ensuite, après avoir donné des applications de cette condition nécessaire et suffisante, les possibilités de



Digitized by the Internet Archive  
in 2026

[https://archive.org/details/IA41551508\\_0041](https://archive.org/details/IA41551508_0041)

construction de tableaux orthogonaux lorsque cette condition n'est pas remplie (Théorèmes II.2.6, II.2.7 et II.2.8).

II.3 expose la méthode des différences [III] et sa généralisation [IX] qui constitue le sujet du théorème II.3.1. Nous donnons ensuite deux applications de ce théorème. En particulier le théorème II.3.3. introduit la notion d'orthomorphisme de groupe [XIII].

II.4 montre comment utiliser les groupes 2 fois transitifs sur un ensemble pour construire des tableaux orthogonaux idempotents de force 2.

II.5 donne enfin deux méthodes de construction utilisant seulement les corps de Galois ([V] et [III]).

Le troisième chapitre est consacré à l'étude des méthodes de construction de tableaux orthogonaux à partir de tableaux orthogonaux déjà existant.

III.1 décrit la méthode de construction "par produit direct".

III.2 expose une modification d'une méthode de Yamamoto [XXII] qui consiste à supprimer des conditions restrictives au prix d'une augmentation de l'indice de 1 à 2 dans le cas des tableaux orthogonaux de force 2. Une première extension de cette méthode modifiée [XIV] portant sur la force du tableau est donnée dans le théorème III.2.1. Une seconde extension portant sur le nombre de lignes au tableau est donnée dans le théorème III.2.2.

III.3 expose une généralisation d'une méthode de Sade ([XV]) et [XIX]) pour la construction de tableaux orthogonaux.

Enfin le quatrième chapitre fait le point sur la majoration des contraintes des tableaux orthogonaux.



Les résultats ont été donnés dans IV.1 pour les tableaux orthogonaux d'indice unité[V] et dans IV.2 pour les tableaux orthogonaux de force 2 et 3[III] . Certaines précisions sur la majoration des contraintes résultent d'applications des méthodes de construction (théorème IV.1.1.).

---



## I - DEFINITIONS ET PROPRIETES ELEMENTAIRES

---

### I.1 - Tableau orthogonal :

Soit  $(a_{ij})$  une matrice de  $r$  lignes ( $i = 1, 2, \dots, r$ ) et de  $N$  colonnes ( $j = 1, 2, \dots, N$ ) dont les éléments appartiennent à l'ensemble  $E = \{e_1, e_2, \dots, e_s\}$ . Soit  $(P)$  la propriété suivante :

toute sous-matrice de  $t$  lignes et  $N$  colonnes ( $t \leq r$ ) extraite de la matrice  $(a_{ij})$  est telle que tous les éléments de  $E^t$  soient représentés chacun à  $\lambda$  exemplaires par les colonnes de cette sous-matrice de  $t$  lignes et  $N$  colonnes.

Si  $(a_{ij})$  possède la propriété  $(P)$ , cette matrice est appelée tableau orthogonal.

Le paramètre  $t$  est appelé force du tableau orthogonal.

Le paramètre  $\lambda$  est appelé indice du tableau orthogonal.

Le paramètre  $r$  est appelé nombre de contraintes du tableau orthogonal.

Un tableau orthogonal ainsi défini est désigné par ses quatre paramètres  $(\lambda, r, s, t)$ .

On remarque que  $N = \lambda s^t$ .

### I.2 - Hypercube :

Le tableau orthogonal  $(\lambda, r, s, t)$  est appelé hypercube si  $\lambda = s^k$ . ( $k$  nombre entier).

### I.3 - Quasi-groupe fini :

L'ensemble  $E$  muni d'une opération  $\phi$  est un quasi-groupe fini noté  $E(\phi)$ , si  $E$  est fini et si quelque soit  $(a, b) \in E^2$  les équations  $x \phi a = b$  et  $a \phi y = b$  ont des solutions uniques dans  $E$  en  $x$  et  $y$ .

$\text{card } E$  est appelé l'ordre du quasi-groupe  $E(\phi)$ .



#### I.4 - Quasi-groupes orthogonaux :

Deux quasi-groupes de même ordre  $E(\phi_1)$  et  $E(\phi_2)$  sont orthogonaux si, quel que soit  $(a,b) \in E^2$ , le système d'équations

$$\begin{cases} x \phi_1 y = a \\ x \phi_2 y = b \end{cases}$$

a une solution unique en  $(x,y)$

#### I.5 - Equivalence de la propriété (P) possédée par des tableaux orthogonaux d'indice unité et d'une propriété analogue à celle des quasi-groupes mutuellement orthogonaux :

Si on considère dans un tableau orthogonal  $(1,r,s,t)$  un ensemble déterminé de  $t$  lignes, les  $t$  premières lignes par exemple :  $l_1, l_2, \dots, l_t$ , on obtient ainsi dans les colonnes tous les éléments de  $E^t$  une fois et une seule. On peut donc se servir de ces éléments de  $E^t$  pour repérer les colonnes du tableau orthogonal. Chaque élément  $a_{i,X}$  de la  $i^{\text{ème}}$  ligne et de la colonne  $X$  peut alors être considéré comme image dans  $E$ , par une application  $f_{1,2,\dots,t}^i$  de  $E^t$  dans  $E$ , de  $X \in E^t$ , soit :

$$a_{i,X} = f_{1,2,\dots,t}^i(X) \quad , \quad X \in E^t$$

avec  $f_{1,2,\dots,t}^i(X) =$  composante de rang  $i$  du  $t$ -uplet  $X$

$$\text{si } i \leq t$$

La propriété caractéristique (P) d'un tableau orthogonal se traduira alors de la façon suivante :

le système d'équations :  $f_{1,2,\dots,t}^{ik}(X) = u_{i_k} \quad (k = 1, 2, \dots, t)$

(et dans lequel  $\{i_k \mid k = 1, 2, \dots, t\} \subset \{1, 2, \dots, r\}$   
et  $u_{i_k} \in E$ ) a une solution unique en  $X$

quelque soit  $(u_{i_1}, u_{i_2}, \dots, u_{i_k}, \dots, u_{i_t}) \in E^t$



Cas particulier d'un tableau orthogonal d'indice unité et de force 2 :

1) Dans le cas où  $i_2 \in \{1, 2\}$ , nous devons avoir :

$$f_{i,2}^{i_1}(x, u_{i_2}) = u_{i_1} \text{ a une solution unique en } x, \forall (u_{i_1}, u_{i_2}) \in E^2$$

2) Dans le cas où  $i_1 \in \{1, 2\}$ , nous devons avoir :

$$f_{1,2}^{i_2}(u_{i_1}, y) = u_{i_2} \text{ a une solution unique en } y, \forall (u_{i_1}, u_{i_2}) \in E^2$$

3) Dans le cas où  $\{i_1, i_2\}_{i, \neq i_2} \cap \{1, 2\} = \emptyset$ , nous devons avoir

$$\left. \begin{array}{l} f_{1,2}^{i_1}(x, y) = u_{i_1} \\ f_{1,2}^{i_2}(x, y) = u_{i_2} \end{array} \right\} \text{ a une solution unique en } (x, y), \forall (u_{i_1}, u_{i_2}) \in E^2$$

Si l'on pose :

$$f_{1,2}^{i_1}(a, b) = a \Phi_1 b$$

$$f_{1,2}^{i_2}(a, b) = a \Phi_2 b$$

les propriétés mises en évidence en 1) et 2) montrent que  $\Phi_1$  et  $\Phi_2$  sont des opérations de quasi-groupes dans E. La propriété mise en évidence en 3) montre que les quasi-groupes  $E(\Phi_1)$  et  $E(\Phi_2)$  sont orthogonaux. Réciproquement si l'on a k quasi-groupes mutuellement orthogonaux

$\{E(\Phi_i) ; 1 \leq i \leq k\}$ , on construit le tableau :

$$\{(x, y, x \Phi_1 y, \dots, x \Phi_i y, \dots, x \Phi_k y) ; \forall (x, y) \in E^2\}$$

qui est un tableau orthogonal  $(1, k+2, s, 2)$ . Il en résulte donc le

Théorème : l'existence d'un ensemble de k quasi-groupes mutuellement orthogonaux d'ordre s est équivalente à celle d'un tableau orthogonal  $(1, k+2, s, 2)$ .



### I.6 - Tableaux orthogonaux isotopes :

Soient un tableau orthogonal  $(\lambda, r, s, t)$  construit sur un ensemble  $E$ , un ensemble de  $r$  permutations de  $E$   $\{\pi_1, \pi_2, \dots, \pi_i, \dots, \pi_r\}$  et une permutation  $\sigma$  de l'ensemble  $\{1, 2, \dots, r\}$ . Soit  $a_{ij}$  l'élément de la  $i^{\text{ème}}$  ligne et de la  $j^{\text{ème}}$  colonne du tableau orthogonal considéré. Considérons le tableau de  $r$  lignes et  $\lambda s^t$  colonnes, dont l'élément de la  $i^{\text{ème}}$  ligne et de la  $j^{\text{ème}}$  colonne est :

$$b_{ij} = \pi_i (a_{ij})$$

(cette opération diffère d'une permutation des colonnes).

On obtient évidemment un nouveau tableau orthogonal  $(\lambda, r, s, t)$ . Enfin, si l'on change les lignes de place dans ce tableau, ce dernier reste orthogonal, c'est-à-dire que si l'on considère le tableau à  $r$  lignes et  $s^t$  colonnes dont l'élément de la  $i^{\text{ème}}$  ligne et de la  $j^{\text{ème}}$  colonne est :

$$c_{ij} = b_{\sigma(i) j} = \pi_{\sigma(i)} (a_{\sigma(i) j})$$

on obtient encore un tableau orthogonal  $(\lambda, r, s, t)$ .

Deux tableaux orthogonaux tels que  $(a_{ij})$  et  $(c_{ij})$  seront appelés isotopes. - ayant remarqué que l'on peut évidemment passer de  $(c_{ij})$  à  $(a_{ij})$  par des opérations analogues à celles qui ont permis de passer de  $(a_{ij})$  à  $(c_{ij})$ .

### I.7 - Sous-tableau d'un tableau orthogonal :

Un tableau orthogonal  $(\lambda, r, s, t)$  étant considéré comme la juxtaposition de ses  $\lambda s^t$  colonnes (certaines pouvant être identiques), on appellera sous-tableau du tableau orthogonal considéré la juxtaposition d'un certain nombre de colonnes de ce tableau (certaines pouvant être identiques).

### I.8 - Transversale d'un quasi-groupe :

Etant donné  $E(\Phi)$  un quasi-groupe d'ordre  $s$ , soit

$$U = \{(x_i, x_j, x_i \Phi x_j) \ , \ \forall (x_i, x_j) \in E^2\} \subset E^3,$$

S'il existe  $T \subset U$ , tel que :

$$T = \{(x_i, x_{\pi(i)}, x_{\sigma(i)}) , \ \forall x_i \in E\}$$



$\pi$  et  $\sigma$  étant des permutations de  $\{1, 2, \dots, s\}$ , on dit que  $T$  est une transversale de  $E(\phi)$ .

Théorème : l'existence de  $s$  transversales deux à deux disjointes de  $E(\phi)$  équivaut à l'existence d'un quasi-groupe  $E(\psi)$  orthogonal à  $E(\phi)$ .

Ce théorème est un cas particulier du théorème démontré dans le prochain paragraphe.

### I.9 - Transversale d'un tableau orthogonal :

Etant donné un tableau orthogonal  $(\lambda, r, s, t)$ , s'il existe un sous-tableau  $T$  du tableau orthogonal considéré, tel que  $T$  soit un tableau orthogonal  $(\lambda, r, s, t-1)$ , le tableau orthogonal  $T$  est appelé transversale du tableau orthogonal considéré.

Théorème : l'existence de  $s$  transversales deux à deux disjointes d'un tableau orthogonal  $(\lambda, r, s, t)$  équivaut à l'existence d'un tableau orthogonal  $(\lambda, r+1, s, t)$ .

En effet, soit  $E = \{e_1, e_2, \dots, e_s\}$  l'ensemble sur lequel est construit le tableau orthogonal  $(\lambda, r, s, t)$ .

Soient  $T_1, T_2, \dots, T_k, \dots, T_s$  les  $s$  transversales deux à deux disjointes du tableau orthogonal  $(\lambda, r, s, t)$ .

Soit  $U_k = (T_k, e_k)$  qui désigne le tableau obtenu à partir de  $T_k$  en ajoutant une ligne à chaque colonne de  $T_k$ , ligne dont l'élément est  $e_k$  quelle que soit la colonne de  $T_k$ .  $T_k$  étant un tableau orthogonal de force  $t-1$ , les  $\lambda s^{t-1}$   $t$ -uples constitués par les  $(t-1)$ -uples correspondant à un ensemble donné de  $(t-1)$  lignes de  $T_k$  et l'élément  $e_k$ , nous fournissent  $\lambda$  fois les éléments  $(X, e_k)$  où  $X$  parcourt  $E^{t-1}$ .

Si  $k$  prend toutes les valeurs  $1, 2, \dots, s$ , on obtient



$k = 1$        $\lambda$  fois       $(X, e_1)$       où  $X$  parcourt  $E^{t-1}$   
 $k = 2$        $\lambda$  fois       $(X, e_2)$       où  $X$  parcourt  $E^{t-1}$   
.....  
 $k = s$        $\lambda$  fois       $(X, e_s)$       où  $X$  parcourt  $E^{t-1}$

C'est-à-dire  $\lambda$  fois  $(X, e_i)$ , où  $X$  parcourt  $E^{t-1}$  et  $e_i$  parcourt  $E$  donc  $\lambda$  fois les éléments de  $E^t$ .

La juxtaposition de  $U_1, U_2, \dots, U_k, \dots, U_s$  forme donc bien un tableau orthogonal  $(\lambda, r+1, s, t)$ .

Réciproquement si l'on considère un tableau orthogonal  $(\lambda, r+1, s, t)$ , on peut le décomposer en  $s$  tableaux  $U_k$  :

$U_k$  = sous-tableau formé des colonnes de  $(\lambda, r+1, s, t)$  dont l'élément de la dernière ligne est  $e_k$ .

On peut alors en déduire  $T_k$  obtenu en supprimant la dernière ligne de  $U_k$ . Les  $s$  tableaux  $T_k$  ainsi obtenus sont des tableaux orthogonaux de force  $(t-1)$  à  $r$  lignes et sont 2 à 2 disjoints puisque les  $U_k$  sont par définition 2 à 2 disjoints. Les  $T_k$  ainsi obtenus forment donc bien  $s$  transversales 2 à 2 disjointes du tableau orthogonal  $(\lambda, r, s, t)$  obtenu à partir du tableau orthogonal  $(\lambda, r+1, s, t)$  en supprimant la dernière ligne.

Si l'on fait  $\lambda = 1, r = 3, t = 2$  on obtient bien, compte tenu du théorème du paragraphe I.5, le théorème du paragraphe précédent.

#### I.10 - Quasi-groupes idempotents :

Le quasi-groupe  $E(\phi)$  est dit idempotent si

$$x \phi x = x, \quad \forall x \in E$$

Théorème : Etant donnés  $m$  quasi-groupes mutuellement orthogonaux, on peut en déduire  $(m-1)$  quasi-groupes mutuellement orthogonaux idempotents.



Ce théorème (dû à MANN) est un cas particulier du théorème démontré dans le prochain paragraphe.

### I.11 - Tableaux orthogonaux idempotents :

Dans le cas de tableaux orthogonaux d'indice  $\lambda = 1$ , il est naturel de dire (en reprenant les notations du paragraphe I.5) que si

$$f_{1,2,\dots,t}^i(X) = x, \text{ chaque fois que}$$

$X = (x, x, \dots, x, \dots, x)$ ,  $X \in E^t$ ,  $\forall x \in E$ ,  $\forall i = 1, 2, \dots, r$  le tableau orthogonal  $(1, r, s, t)$  considéré est idempotent.

(Cette définition équivaut dans le cas  $t = 2$  à celle d'un ensemble de quasi-groupes idempotents mutuellement orthogonaux). On dira, par extension, quelque soit l'indice  $\lambda$ , que le tableau orthogonal  $(\lambda, r, s, t)$  est idempotent si l'égalité de  $t$  éléments d'une colonne entraîne l'égalité de tous les éléments de la colonne considérée.

Théorème : Etant donné un tableau orthogonal  $(1, r + t - 1, s, t)$ , on peut en déduire un tableau orthogonal  $(1, r, s, t)$  idempotent.

En effet, soit  $E = \{e_1, e_2, \dots, e_s\}$  l'ensemble sur lequel est construit le tableau orthogonal  $(1, r + t - 1, s, t)$ . Considérons le sous-tableau  $T$  défini par la condition que tous les éléments situés dans les  $(t-1)$  premières lignes de ses  $s$  colonnes soient égaux à  $e_1$ . Si nous supprimons alors les  $(t-1)$  premières lignes du tableau  $T$ , nous obtenons un tableau  $U$  de  $r$  lignes et  $s$  colonnes et ce tableau  $U$  est un tableau orthogonal  $(1, r, s, 1)$ . Cela entraîne que ses colonnes sont de la forme :

$$[e_i, \pi_1(e_i), \pi_2(e_i), \dots, \pi_k(e_i), \dots, \pi_{r-1}(e_i)]$$

où  $\pi_1, \pi_2, \dots, \pi_k, \dots, \pi_{r-1}$  sont  $r - 1$  permutations de  $E$ .

$U$  est un sous-tableau du tableau orthogonal  $V(1, r, s, t)$  obtenu en supprimant les  $(t-1)$  premières lignes du tableau orthogonal  $(1, r + t - 1, s, t)$  que nous nous sommes donné. Transformons  $V$  en  $W(1, r, s, t)$  par l'isotopie qui consiste à appliquer aux éléments de la  $(K+1)^{\text{ème}}$  ligne la permutation  $\pi_k^{-1}$ ,  $\forall k = 1, 2, \dots, r-1$ .



Le sous-tableau U de V est transformé en un sous-tableau U' de W dont les colonnes sont de la forme :

$$[e_i, e_i, e_i, \dots, e_i, \dots, e_i]$$

le tableau orthogonal W (1, r, s, t) ainsi construit est donc bien un tableau orthogonal idempotent.

Si l'on fait  $t = 2$ ,  $r = m+1$ , on obtient bien, compte tenu du paragraphe I.5 le théorème du paragraphe précédent.

#### I.12 - Sous-quasi-groupe d'un quasi-groupe fini :

Etant donné un quasi-groupe fini  $E(\Phi)$ , s'il existe une partie F de E telle que  $a \Phi b \in F$ ,  $\forall (a, b) \in F^2$ , on dit que F est un sous-quasi-groupe du quasi-groupe  $E(\Phi)$ .

On note ce quasi-groupe  $F(\Phi)$ .

(dans le cas fini, la seule condition énoncée ci-dessus entraîne pour F les autres propriétés caractéristiques des quasi-groupes).

Théorème : Etant donnés s et  $s_1 \leq s$  et m quasi-groupes mutuellement orthogonaux construits sur E d'ordre s, si chacun de ces m quasi-groupes mutuellement orthogonaux contient un sous-quasi-groupe construit sur  $F \subseteq E$  d'ordre  $s_1$ , tel que les m sous-quasi-groupes d'ordre  $s_1$  soient mutuellement orthogonaux, alors  $s \geq (m+1) s_1$

Théorème : Sous les hypothèses du théorème précédent, s'il existe un  $(m+1)^{\text{ème}}$  quasi-groupe d'ordre s construit sur E, alors :

$$s_1 \leq \frac{s - s_1}{m+1} + \text{partie entière de } \left( \frac{s_1^2}{s} \right)$$

Théorème : Etant donnés s et  $s_1 \leq s$  et  $(s_1 - 1)$  quasi-groupes mutuellement orthogonaux construits sur E, d'ordre s, si chacun de ces  $(s_1 - 1)$  quasi-groupes d'ordre  $s_1$  contient un sous-quasi-groupe d'ordre  $s_1$ , construit sur  $F \subseteq E$ , de telle façon que les  $(s_1 - 1)$  sous-quasi-groupes d'ordre  $s_1$  soient mutuellement orthogonaux, et s'il existe un  $s_1^{\text{ème}}$  quasi-groupe d'ordre s construit sur E,



orthogonal aux  $(s_1 - 1)$  quasi-groupes d'ordre  $s$ , construits sur  $E$ , alors

$$s \geq s_1^2$$

et si  $s > s_1^2$  alors  $s \geq s_1^2 + s_1$

Ces 3 théorèmes sont respectivement des cas particuliers des 3 théorèmes démontrés dans le prochain paragraphe.

I.13 - Sous-tableau orthogonal  $(\lambda, r, s_1, t)$  d'un tableau orthogonal  $(\lambda, r, s, t)$  ( $s \geq s_1$ ) :

Etant donné un tableau orthogonal  $(\lambda, r, s, t)$  construit sur un ensemble  $E$ , s'il existe  $\lambda s_1^t$  colonnes de ce tableau dont les éléments appartiennent à  $F \subseteq E$  et à  $F$  seulement et dont la juxtaposition constitue un tableau orthogonal  $(\lambda, r, s_1, t)$ , on dit que le tableau orthogonal  $(\lambda, r, s_1, t)$  est un sous-tableau orthogonal du tableau orthogonal  $(\lambda, r, s, t)$

Théorème : Etant donné un tableau orthogonal  $(1, r, s, t)$  construit sur  $E$ , possédant un sous-tableau orthogonal  $(1, r, s_1, t)$  construit sur  $F \subseteq E$ , ( $s_1 \leq s$ ), on a l'inégalité :

$$s \geq (r - t + 1) s_1$$

Soit  $F = \{e_1, e_2, \dots, e_{s_1}\}$

et  $C_E^F = \{e_{s_1+1}, e_{s_1+2}, \dots, e_s\}$

Avec les notations du paragraphe I.5, on a :

$$f_1, 2, \dots, t(X) \in F, \forall i \in \{1, 2, \dots, r\}, \forall X \in F^t$$

puisque le tableau orthogonal  $(1, r, s, t)$  admet un sous-tableau orthogonal  $(1, r, s_1, t)$  construit sur  $F$ .



$$f_1^i, 2, \dots, t(X) \in \binom{F}{E} \quad \forall i \in \{t+1, t+2, \dots, r\}$$

si  $X$  est tel qu'une et une seule de ses composantes appartient à  $\binom{F}{E}$  et les  $(t-1)$  autres composantes appartiennent à  $F$ . En effet s'il existait un  $i \in \{t+1, t+2, \dots, r\}$  et tel que  $f_1^i, 2, \dots, t(X) \in F$ , alors il existerait une colonne dont  $t$  éléments appartiendraient à  $F$ , sans que les autres appartiennent à  $F$  ce qui est impossible d'après la définition même du sous-tableau orthogonal construit sur  $F$ .

- Considérons maintenant  $X$  tel que 2 et 2 seulement de ses composantes, par exemple celles de rang  $(t-1)$  et  $t$  appartiennent à  $\binom{F}{E}$ . Soit donc  $T_{t-2}$  l'ensemble des colonnes telles que les  $(t-2)$  premières composantes appartiennent à  $F$  et dont les  $(t-1)^{\text{ème}}$  et  $t^{\text{ème}}$  composantes appartiennent à  $\binom{F}{E}$ . Pour la même raison que ci-dessus, ou bien il existe un  $i$  et un seul de  $\{t+1, t+2, \dots, r\}$  tel que  $f_1^i, 2, \dots, t(X) \in F$  ou bien il n'en existe pas. Soit donc  $T_{t-2, i} \subset T_{t-2}$  l'ensemble des colonnes de  $T_{t-2}$  telles que la composante de rang  $i$  appartient à  $F$  et  $T_{t-2, 0} \subset T_{t-2}$  l'ensemble de celles dont toutes les composantes de rang  $\geq t+1$  appartiennent à  $\binom{F}{E}$ .

Nous avons :

$$\begin{aligned} \text{Card}(T_{t-2, i}) &+ n^{\text{bre}} \text{ de colonnes du sous-tableau construit sur } F \\ &= n^{\text{bre}} \text{ de } t\text{-uplets dont les composantes } 1, 2, \dots, t-2, i \text{ appartiennent} \\ &\text{à } F \text{ et celle de rang } (t-1) \text{ est quelconque} = s_1^{t-1} s \end{aligned}$$

$$\text{ce qui donne } \text{card}(T_{t-2, i}) = s_1^{t-1} s - s_1^t = s_1^{t-1} (s - s_1) \quad \forall i \geq t+1$$

Le fait que  $T_{t-2, 0}$  et les  $T_{t-2, i}$  sont 2 à 2 disjoints et que

$$T_{t-2} = T_{t-2, 0} \cup \left( \bigcup_i T_{t-2, i} \right) \text{ entraîne}$$

$$\text{que } \text{card}(T_{t-2}) = \text{card}(T_{t-2, 0}) + \sum_{i=t+1}^r \text{card}(T_{t-2, i})$$

$$\text{soit } s_1^{t-2} (s - s_1)^2 = \text{card}(T_{t-2, 0}) + (r - t) s_1^{t-1} (s - s_1)$$

$$\text{donc } \text{card}(T_{t-2, 0}) = s_1^{t-2} (s - s_1)^2 - (r - t) s_1^{t-1} (s - s_1)$$

nous devons donc avoir

$$s_1^{t-2} (s - s_1)^2 - (r - t) s_1^{t-1} (s - s_1) \geq 0$$



Soit encore

$$s - s_1 \gg (r - t) s_1$$

soit

$$s \gg (r - t + 1) s_1$$

Si l'on fait  $t = 2$  et  $r = m + 2$ , on trouve le théorème du paragraphe précédent.

Théorème : Etant donné un tableau orthogonal  $(1, r, s, t)$  construit sur  $E$ , possédant un sous-tableau orthogonal  $(1, r, s_1, t)$  construit sur  $F \subseteq E$  ( $s_1 \leq s$ ), si l'on peut ajouter au tableau orthogonal  $(1, r, s, t)$  une  $(r + 1)^{\text{ème}}$  ligne pour en faire un tableau orthogonal  $(1, r + 1, s, t)$  alors :

$$s_1 \leq \frac{s - s_1}{r - t + 1} + (\text{partie entière de } \frac{s_1^t}{s}) / s_1^{t-2}$$

Considérons  $T$  une des  $s$  transversales 2 à 2 disjointes du tableau orthogonal  $(1, r, s, t)$  (ces transversales existent en vertu du théorème du paragraphe I.9). Soit  $d$  le nombre de colonnes dont les éléments appartiennent à  $F$  et à  $F$  seulement. Soit  $a_1$  le nombre de colonnes telles que les  $(t-1)$  premières composantes appartiennent à  $F$  et celle de rang  $t$  appartienne à  $\binom{F}{E}$ . Soit enfin  $a_2$  le nombre de colonnes telles que les  $(t-2)$  premières composantes appartiennent à  $F$  et celles de rang  $(t-1)$  et  $t$  appartiennent à  $\binom{F}{E}$ .

Le dénombrement des  $(t-1)$ -uplets dont les  $(t-1)$  composantes sont celles des  $(t-1)$  premières lignes et appartiennent à  $F$  donne :

$$s_1^{t-1} = d + a_1, \text{ soit } a_1 = s_1^{t-1} - d$$

Soit

$$\left\{ \text{colonnes dont les } (t-2) \text{ premiers éléments appartiennent à } F \right\} = A$$



$$\left\{ \begin{array}{l} \text{colonnes dont les } (t-2) \text{ premiers éléments appartiennent à } F, \\ \text{dont le } (t-1)^{\text{ème}} \text{ appartient à } \binom{F}{E}, \\ \text{et dont le } t^{\text{ème}} \text{ appartient à } \binom{F}{E} \end{array} \right\} = A_{00}$$

$$\left\{ \begin{array}{l} \text{colonnes dont les } (t-2) \text{ premiers éléments appartiennent à } F, \\ \text{dont le } (t-1)^{\text{ème}} \text{ appartient à } \binom{F}{E}, \\ \text{et dont le } t^{\text{ème}} \text{ appartient à } F \end{array} \right\} = A_{01}$$

$$\left\{ \begin{array}{l} \text{colonnes dont les } (t-2) \text{ premiers éléments appartiennent à } F, \\ \text{dont le } (t-1)^{\text{ème}} \text{ appartient à } F \\ \text{et dont le } t^{\text{ème}} \text{ appartient à } \binom{F}{E} \end{array} \right\} = A_{10}$$

$$\left\{ \text{colonnes dont les } t \text{ premiers éléments appartiennent à } F \right\} = A_{11}$$

Les parties de  $A : A_{00}, A_{01}, A_{10}, A_{11}$ , lorsqu'elles ne sont pas vides forment une partition de  $A$  et l'on a :

$$\text{Card } A = \text{card } (A_{00}) + \text{card } (A_{01}) + \text{card } (A_{10}) + \text{card } (A_{11})$$

$$\text{soit } ss_1^{t-2} = a_2 + a_1 + a_1 + d$$

$$\text{soit encore } a_2 = ss_1^{t-2} - 2 s_1^{t-1} + d$$

Or, il est impossible que les colonnes dont les  $(t-2)$  premiers éléments appartiennent à  $F$ , les  $(t-1)^{\text{ème}}$  et  $t^{\text{ème}}$  appartenant à

$\binom{F}{E}$ , aient parmi leurs autres composantes plus d'un élément appartenant à  $F$ . Il en résulte :

$$a_2 \geq \sum_{k=t+1}^{k=r} \text{card} \left\{ \text{colonnes telles que les } (t-2) \text{ premières composantes appartiennent à } F, \text{ la } k^{\text{ème}} \text{ appartient à } F \text{ et les autres appartiennent à } \binom{F}{E} \right\}$$



Il découle de la structure du tableau orthogonal initial dont T est une transversale que si :

$$X = (x_1, x_2, \dots, x_t) \text{ et } k \geq t+1,$$

$$f_{1,2,\dots,t}^k(X) \notin F \text{ si } x_j \in F \text{ pour } 1 \leq j \leq t-1 \text{ et } x_t \notin F$$

$$f_{1,2,\dots,t}^k(X) \notin F \text{ si } x_j \in F \text{ pour } 1 \leq j \leq t-2 \text{ et pour } j = t \text{ et } x_{t-1} \notin F$$

(début de la démonstration du précédent théorème)

et donc le dénombrement des colonnes de T ayant leurs (t-2) premiers éléments appartenant à F et le k<sup>ème</sup> appartenant à F, donne :

$$s_1^{t-1} = \text{card} \left\{ \begin{array}{l} \text{colonnes telles que les (t-2) premières composantes} \\ \text{appartiennent à F, la k<sup>ème</sup> appartient à F, les autres} \\ \text{appartiennent à } \begin{pmatrix} F \\ E \end{pmatrix} \end{array} \right\}$$

+ d

L'inégalité à laquelle nous avons abouti précédemment s'écrit donc :

$$a_2 \geq \sum_{k=t+1}^{k=r} (s_1^{t-1} - d)$$

$$\text{soit } a_2 \geq (s_1^{t-1} - d)(r - t)$$

$$\text{ou } s s_1^{t-2} - 2 s_1^{t-1} + d \geq (s_1^{t-1} - d)(r - t)$$

$$\text{et } d \geq s_1^{t-1} - s_1^{t-2} \frac{s-s_1}{r-t+1}$$

A chaque transversale T correspond une valeur d, soit en tout s valeurs de d :  $d_1, d_2, \dots, d_s$  telles que

$$s_1^t = d_1 + d_2 + \dots + d_s \text{ et soit } d_q \text{ de } T_q \text{ telle}$$



que  $d_q \leq \frac{s_1^t}{s}$ , on aura alors :

$$\text{partie entière de } \left( \frac{s_1^t}{s} \right) \geq s_1^{t-1} - s_1^{t-2} \frac{s - s_1}{r - t + 1}$$

qui entraîne bien l'inégalité que nous avons à démontrer.

Si l'on fait  $t = 2$  et  $r = m + 2$ , on trouve bien le 2ème théorème du paragraphe I.12 comme cas particulier.

Théorème : Etant donné un tableau orthogonal  $(1, t+s_1 - 1, s, t)$  construit sur  $E$ , possédant un sous-tableau orthogonal  $(1, t+s_1 - 1, s_1, t)$  construit sur  $F \subseteq E$  ( $s_1 \leq s$ ), si l'on peut ajouter au tableau orthogonal  $(1, t+s_1 - 1, s, t)$  une nouvelle ligne pour en faire un tableau orthogonal  $(1, t+s_1, s, t)$  alors :

$$\underline{s \geq s_1^2}$$

Dans le cas particulier où  $t = 2$ , ou bien  $s = s_1^2$   
ou bien  $\underline{s \geq s_1^2 + s_1}$

La première partie du théorème est un simple corollaire du 1er théorème de ce paragraphe dans lequel on fait :

$r = t + s_1 - 1$ . Dans le cas particulier  $t = 2$ , la partie entière de  $\frac{s_1^2}{s}$  est nulle dès lors que  $s \neq s_1^2$  (d'après la première partie du théorème). Il en résulte l'inégalité

$$s_1 \leq \frac{s - s_1}{r - t + 1} \quad (\text{compte tenu du 2ème théorème de}$$

ce paragraphe) et donc puisque  $r - t + 1 = s_1$ ,  $s \geq s_1^2 + s_1$



II - Les méthodes de construction de  
tableaux orthogonaux utilisant les groupes finis

II.1 - Les groupes sous-transitifs : définitions et propriétés  
générales (XI)

Définition II.1.1. - Soient  $G_i$  ( $i = 1, 2, \dots, r$ )  $r$  groupes de substitutions opérant chacun sur le même ensemble de lettres  $E$  ( $\text{card } E = s$ ) et transitifs sur  $E$ . Un sous-groupe  $H$  du produit cartésien  $G_1 \times G_2 \times \dots \times G_r$  opérant sur  $E^r$  sera dit sous-transitif d'ordre  $t \leq r$  sur  $E^r$  s'il possède la propriété suivante :

étant donné un élément de  $E^r$ ,  $A = (a_1, a_2, \dots, a_r)$  et un élément de  $E^t$ ,  $A' = (a_{i_1}, a_{i_2}, \dots, a_{i_t})$  extrait de  $A$

$(\{i_1, i_2, \dots, i_t\} \subset \{1, 2, \dots, r\})$  et  $i_1 < i_2 < \dots < i_t$

et un élément quelconque de  $E^t$ ,  $B' = (b_{i_1}, b_{i_2}, \dots, b_{i_t})$ , il existe au moins un élément  $\alpha \in H$  et un élément

$B = (b_{i_1}, b_{i_2}, \dots, b_{i_r})$  de  $E^r$  tels que  $\alpha(A) = B$  et que  $B'$

soit extrait de  $B$  (c'est-à-dire que  $b_{i_1}$  occupe le rang  $i_1$  dans  $B$ ,  $b_{i_2}$  occupe le rang  $i_2, \dots, b_{i_t}$  occupe le rang  $i_t$ )

et ceci quels que soient  $A \in E^r$ ,  $A' \in E^t$  extrait de  $A$  et  $B' \in E^t$

Définition II.1.2 : Un complexe de  $G_1 \times G_2 \times \dots \times G_r$  possédant la propriété énoncée dans la définition II.1.1. est aussi dit sous-transitif d'ordre  $t$  sur  $E^r$ .



Théorème II.1.1. : si un sous-groupe  $H$  du produit cartésien  $G_1 \times G_2 \times \dots \times G_r$  ( $G_i$  groupe transitif opérant sur l'ensemble de lettres  $E$ ) est sous-transitif d'ordre  $t$  sur  $E^r$  ( $\text{card } E = s$ ), alors l'ordre de  $H$  est un multiple de  $s^t$ , soit :

$$[H] = \lambda s^t, \lambda \text{ étant un nombre entier.}$$

Démonstration : Soit  $H'$  le sous-groupe de  $G_1 \times G_2 \times \dots \times G_t$  induit par  $H$  sur les  $t$  premières composantes.

L'application qui à  $h = (h_1, h_2, \dots, h_r) \in H$  fait correspondre  $h' = (h_1, h_1, \dots, h_t) \in H'$  est un homomorphisme de  $H$  sur  $H'$ . Le noyau de cet homomorphisme est l'ensemble  $N$  des éléments de  $H$  dont les  $t$  premières composantes sont égales à l'unité donc  $H' \cong H/N$ . En vertu de la sous-transitivité d'ordre  $t$  de  $H$  sur  $E^r$ ,  $H'$  est transitif sur  $E^t$  donc

$$[H'] = \lambda_1 s^t \quad (\lambda_1 \text{ nombre entier})$$

et il s'en suit que  $[H] = [N] \cdot \lambda_1 s^t = \lambda s^t$

Définition II.1.3 : Etant donné un groupe  $H$  sous-transitif d'ordre  $t$  sur  $E^r$  ( $\text{card } E = s$ ), le nombre  $\lambda = \frac{\text{ordre de } H}{s^t}$  est appelé l'indice de  $H$ .

Théorème II.1.2 : L'existence d'un sous-groupe  $H$  du produit cartésien  $\prod_{i=1}^r G_i$  ( $G_i$  groupe transitif sur l'ensemble  $E$  tel que  $\text{card } E = S$ ) sous-transitif d'ordre  $t$  sur  $E^r$  entraîne l'existence d'un tableau orthogonal  $(\lambda, r, S, t)$ ,  $\lambda$  étant l'indice de  $H$ .

Démonstration : En effet, il suffit d'appliquer à un élément quelconque de  $E^r$  les  $\lambda s^t$  éléments de  $H$  et de juxtaposer les



résultats obtenus. On obtient un tableau orthogonal  $(\lambda, r, s, t)$  il suffit de considérer un t-uple  $T$  occupant la place  $P$  dans un r-uple  $V$  et lorsqu'on applique à  $V$  tous les éléments de  $H$ , on obtient des r-uples dont la place  $P$  est occupée par tous les t-uples possibles, chacun étant répété  $\lambda$  fois.

Théorème II.1.3 : Soit  $H$  un sous-groupe du produit cartésien  $\prod_{i=1}^r G_i$ , les  $G_i$  étant des groupes de substitutions opérant sur le même ensemble de lettres  $E$ .

Soient  $H_i$  le sous-groupe de  $G_i$  induit par  $H$  sur  $E$

$H_{\bar{i}}$  le sous-groupe de  $\prod_{j=1}^r G_j (j \neq i)$  induit par  $H$  sur  $E^{r-1}$

$h_i$  le sous-groupe de  $H_i$  formé des éléments de  $G_i$  intervenant dans  $H$  avec les éléments unités des autres groupes  $G_j$

$h_{\bar{i}}$  le sous-groupe de  $H_{\bar{i}}$  formé des éléments de  $\prod_{j=1}^r G_j (j \neq i)$  intervenant dans  $H$  avec l'élément unité de  $G_i$

alors  $h_i$  est normal dans  $H_i$  et  $h_{\bar{i}}$  est normal dans  $H_{\bar{i}}$ .

De plus  $H_i/h_i$  et  $H_{\bar{i}}/h_{\bar{i}}$  sont isomorphes. On peut donc écrire

$$H_i = \sum_1 h_i u_1 \quad \text{et} \quad H_{\bar{i}} = \sum_1 h_{\bar{i}} v_1 \quad \text{où } h_i u_1 \text{ correspond à } h_{\bar{i}} v_1$$

dans l'isomorphisme. Enfin, les éléments de  $H$  sont de la forme  $(g_1, g_2)$  où  $g_1 \in h_i u_1$  et  $g_2 \in h_{\bar{i}} v_1$ .

[ Dans la suite, nous exprimerons cette dernière propriété en disant :  
"H résulte du produit d'une classe de  $h_i$  dans  $H_i$  par la classe correspondante de  $h_{\bar{i}}$  dans  $H_{\bar{i}}$ " ]

Démonstration : Soit  $(1, \dots, 1, a_i, 1, \dots, 1)$  un élément de  $H$  intervenant avec les éléments unités des  $G_j$  pour  $j \neq i$ .



Soit  $b_i$  un élément de  $H_i$ . Il existe  $b_1, b_2, \dots, b_{i-1}, b_{i+1}, \dots, b_r$  appartenant respectivement à  $G_1, G_2, \dots, G_{i-1}, G_{i+1}, \dots, G_r$ , tels que  $b = (b_1, b_2, \dots, b_{i-1}, b_i, b_{i+1}, \dots, b_r) \in H$  et

on a :  $b^{-1} (1, 1, \dots, 1, a_i, 1, \dots, 1) b = (1, \dots, 1, b_i^{-1} a_i b_i, 1, \dots, 1)$   
et donc  $b_i^{-1} a_i b_i \in h_i$  ce qui prouve que le sous-groupe  $h_i$  est normal dans  $H_i$ .

On démontrerait de la même façon que  $h_{\bar{i}}$  est normal dans  $H_{\bar{i}}$ .

Etant donné  $a_i \in H_i$ , l'ensemble des éléments  $(a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_r) \in H_{\bar{i}}$  intervenant avec  $a_i$  dans  $H$  est une classe de  $h_{\bar{i}}$  dans  $H_{\bar{i}}$  et de la même façon l'ensemble des éléments  $a'_i \in H_i$  intervenant dans  $H$  avec un élément donné  $(a'_1, a'_2, \dots, a'_{i-1}, a'_{i+1}, \dots, a'_r) \in H_{\bar{i}}$  est une classe de  $h_i$  dans  $H_i$ . Donc si :

$(a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_r) \in H$ , alors tous les éléments  $(a'_1, a'_2, \dots, a'_{i-1}, a'_i, a'_{i+1}, \dots, a'_r)$  où  $(a'_1, a'_2, \dots, a'_{i-1}, a'_{i+1}, \dots, a'_r) \in h_{\bar{i}} (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_r)$  et  $a'_i \in h_i a_i$

appartiennent à  $H$  et il n'existe pas d'élément

$$(\alpha_1, \alpha_2, \dots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \dots, \alpha_r) \in H \text{ où}$$

ou bien

$$\left\{ \begin{array}{l} (\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_r) \notin h_{\bar{i}} (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_r) \\ \text{et } \alpha_i \in h_i a_i \end{array} \right.$$

ou bien

$$\left\{ \begin{array}{l} (\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_r) \in h_{\bar{i}} (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_r) \\ \text{et } \alpha_i \notin h_i a_i \end{array} \right.$$



Donc pour chaque  $(a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_r) \in H$ , on a déterminé une correspondance biunivoque :

$$h_i a_i \rightleftharpoons h_{\bar{i}} (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_r)$$

entre une classe de  $h_i$  dans  $H_i$  et une classe de  $h_{\bar{i}}$  dans  $H_{\bar{i}}$ .

Enfin si  $(a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_r) \in H$  et

$(b_1, b_2, \dots, b_{i-1}, b_i, b_{i+1}, \dots, b_r) \in H$ , alors

$(a_1 b_1, a_2 b_2, \dots, a_{i-1} b_{i-1}, a_i b_i, a_{i+1} b_{i+1}, \dots, a_r b_r) \in H$ ,

Cette correspondance biunivoque conserve les produits et est un isomorphisme entre les groupes quotients  $H_i/h_i$  et  $H_{\bar{i}}/h_{\bar{i}}$ .

Théorème II.1.4 : Etant donné un groupe  $H'$  sous-groupe de

$\prod_{i=1}^{r-1} G_i$  sous-transitif d'ordre 1 sur  $E^{r-1}$  (les  $G_i$  étant transitifs

sur  $E$ ), une condition nécessaire et suffisante pour que l'on puisse construire un groupe  $H$ , de même ordre que  $H'$ , sous-groupe de

$\prod_{i=1}^r G_i$ , sous-transitif d'ordre 1 sur  $E^r$  et dont la restriction

aux  $r-1$  premières composantes soit  $H'$ , est qu'il existe un sous-groupe normal  $\mathcal{N}_H$  de  $H'$  tel que  $H'/\mathcal{N}_H$  soit isomorphe à un groupe de substitutions transitif sur  $E$ .

Démonstration : La condition est nécessaire : soit  $G_r$  un groupe de substitutions transitif sur  $E$ . Nous essayons de construire

$H \subset \prod_{i=1}^r G_i$ , sous-transitif d'ordre 1 sur  $E^r$  et tel que  $H_{\bar{r}}$  soit confondu avec  $H'$ . D'après le théorème II.1.3, il faut trouver un

sous-groupe normal  $\mathcal{N}_H$  de  $H'$  et un sous-groupe normal  $\mathcal{N}_{G_r}$  de  $G_r$

tels que  $H'/\mathcal{N}_H \cong G_r/\mathcal{N}_{G_r}$  et alors  $H$  est le résultat du produit

d'une classe de  $\mathcal{N}_H$  dans  $H'$  par la classe correspondante de

$\mathcal{N}_{G_r}$  dans  $G_r$ .



Si l'on pose  $[H'] = \lambda s$  ( $\text{card } E = s$ ), nous avons d'après le procédé de construction  $[H] = \lambda s [\mathcal{N}_{G_r}]$ . Puisque  $[H] = \lambda s$ , c'est que  $[\mathcal{N}_{G_r}] = 1$ . donc  $\mathcal{N}_{G_r} = \{1\}$  et donc que l'on a  $H'/\mathcal{N}_H \cong G_r$ .

La condition est suffisante : s'il existe  $\mathcal{N}_H$ , tel que  $H'/\mathcal{N}_H$ , soit isomorphe à  $G_r$  groupe de substitutions transitif sur  $E$ , construisons le groupe

$$\left\{ (g_1, g_2) ; g_1 \in \text{classe de } \mathcal{N}_H, \text{ dans } H' ; \text{ pour toute classe de } \mathcal{N}_H, \text{ dans } H' , g_2 \in G_r \right\}$$

le groupe ainsi construit est bien sous-transitif d'ordre 1. Son ordre est bien le même que celui de  $H'$ .

Théorème II.1.5 : Etant donné un groupe  $H'$  sous-groupe de  $\prod_{i=1}^{r-1} G_i$ , sous-transitif d'ordre  $t$  sur  $E^{r-1}$  (les  $G_i$  étant transitifs sur  $E$ ), une condition nécessaire et suffisante pour qu'on puisse construire un groupe  $H$  de même ordre que  $H'$ , sous-groupe de  $\prod_{i=1}^r G_i$ , sous-transitif d'ordre  $t$  sur  $E^r$  et tel que sa restriction aux  $(r-1)$  premières composantes soit  $H'$ , est qu'il existe un sous-groupe normal  $\mathcal{N}_H$ , de  $H'$  tel que  $H'/\mathcal{N}_H$ , soit isomorphe à un groupe de substitutions  $G_r$  transitif sur  $E$  et que le sous-groupe de  $H'$  formé de l'union des classes de  $\mathcal{N}_H$ , dans  $H'$  images des éléments d'un sous-groupe  $K$  de  $G_r$  fixant une lettre quelconque de  $E$  soit sous-transitif d'ordre  $(t-1)$ .

Démonstration : Le théorème II.1.4 nous montre tout d'abord qu'il doit exister  $\mathcal{N}_H$ , sous-groupe normal de  $H'$  tel que  $H'/\mathcal{N}_H$ , soit isomorphe à un groupe de substitutions transitif sur  $E$  :  $G_r$ .  $H$  résulte alors du produit de chaque classe de  $\mathcal{N}_H$ , dans  $H'$  par l'élément de  $G_r$  correspondant dans cet isomorphisme.

Soit alors  $K_1 = \{e_1, e_2, \dots, e_u\}$  le sous-groupe de  $G_r$  qui fixe la lettre  $a_1$  de  $E$ . L'ensemble des éléments de  $G_r$  qui transforment  $a_1 \in E$  en  $a_j \in E$  est alors constitué par les éléments de  $\alpha_j K_1$  classe de  $K_1$  dans  $G_r$  ( $j = 2, 3, \dots, s$ ).



Dans l'isomorphisme  $H'/\mathcal{N}_H \cong G_r$  les éléments correspondant à  $e_1, e_2, \dots, e_u$  respectivement sont :  $\mathcal{N}_H, e_2' \mathcal{N}_H, \dots, e_u' \mathcal{N}_H$  ; et ceux correspondant aux éléments de  $\alpha_j K_1$  (dans l'ordre  $\alpha_j, \alpha_j e_2, \dots, \alpha_j e_u$ ) sont respectivement :

$$\alpha_j' \mathcal{N}_H, \alpha_j' e_2' \mathcal{N}_H, \dots, \alpha_j' e_u' \mathcal{N}_H.$$

En effet,  $\alpha_j$  correspondant à  $\alpha_j' \mathcal{N}_H$ , dans l'isomorphisme  $\alpha_j e_2$  correspond à  $\alpha_j' \mathcal{N}_H \cdot e_2' \mathcal{N}_H = \alpha_j' e_2' \mathcal{N}_H$ , etc...

Soit  $A_1 = \mathcal{N}_H \cup e_2' \mathcal{N}_H \cup \dots \cup e_u' \mathcal{N}_H$ .

Si  $H$  est sous-transitif d'ordre  $t$ ,  $A_1$  étant l'ensemble des éléments de  $H'$  intervenant avec l'ensemble  $K_1$  des éléments de  $G_r$  qui fixent  $a_1 \in E$ ,  $A_1$  doit être sous-transitif d'ordre  $(t-1)$ . On remarque que  $A_1$  est un sous-groupe de  $H'$ .

Montrons qu'alors  $\alpha_j' \mathcal{N}_H \cup \alpha_j' e_2' \mathcal{N}_H \cup \dots \cup \alpha_j' e_u' \mathcal{N}_H = \alpha_j' A_1$  est un complexe de  $H'$ , sous-transitif d'ordre  $(t-1)$  sur  $E^{r-1}$ . Étant donné  $V$ ,  $(t-1)$ -uple de  $E^{t-1}$ , occupant la place  $P$  dans un  $(r-1)$ -uple  $W$  de  $E^{r-1}$ , et un  $(t-1)$ -uple  $V'$  de  $E^{t-1}$  arbitraire, soit  $V'' = (\alpha_j')^{-1}(V')$  restriction de  $(\alpha_j')^{-1}$  à  $V'$  occupant la place  $P$  dans n'importe quel  $(r-1)$ -uple de  $E^{r-1}$ .  $A_1$  étant sous-transitif d'ordre  $(t-1)$ , il existe  $\beta \in A_1$  tel que  $\beta(W) = W'' \in E^{r-1}$  et que  $V''$  occupe la place  $P$  dans  $W''$  et alors  $\alpha_j' \beta(W) = \alpha_j' (W'') = W' \in E^{r-1}$ , tel que la place  $P$  est occupée par  $V'$  dans  $W'$ . Le complexe  $\alpha_j' A_1$  est donc bien sous-transitif d'ordre  $(t-1)$  sur  $E^{r-1}$ ,  $\forall j = 2, \dots, s$ . Si nous nous attachons successivement aux lettres  $a_1, a_2, \dots, a_s$  de  $E$ , nous obtenons  $S$  conditions nécessaires analogues à la condition " $A_1$  sous-transitif d'ordre  $(t-1)$  sur  $E^{r-1}$ " et il est alors évident que l'ensemble de ces conditions est suffisant pour que  $H$  soit sous-transitif d'ordre  $t$  sur  $E^r$ . Mais nous allons montrer que la seule condition " $A_1$  sous-transitif d'ordre  $(t-1)$  sur  $E^{r-1}$ " entraîne toutes les conditions analogues relatives à  $A_2$ , etc...,  $A_s$ . Il suffit de remarquer que  $A_2$  par exemple est un sous-groupe conjugué de  $A_1$  dans  $H'$ , soit :

$$A_2 = \gamma' A_1 \gamma'^{-1}, \quad \gamma' \in H'$$



En effet dans  $G_r$ ,  $K_2$  sous-groupe qui fixe  $a_2 \in E$  est évidemment conjugué de  $K_1$  :  $K_2 = \gamma K_1 \gamma^{-1}$  ( $\gamma \in G_r$  est telle qu'elle transforme  $a_1$  en  $a_2$ ). Dans l'isomorphisme  $\gamma \rightarrow \gamma' \mathcal{H}_{H'}$  et

$\left\{ (\gamma' \mathcal{H}_{H'}) (e_k' \mathcal{H}_{H'}) (\gamma' \mathcal{H}_{H'})^{-1}, \forall k = 1, 2, \dots, u \right\}$  est l'image de  $K_2$  dans  $H' / \mathcal{H}_{H'}$ . Il en résulte que  $A_2 = \bigcup_{k=1}^u \gamma' e_k' \mathcal{H}_{H'} \gamma'^{-1}$

donc que  $A_2 = \gamma' A_1 \gamma'^{-1}$ . Or nous avons montré que si  $A_1$  est un complexe sous-transitif d'ordre  $(t-1)$  sur  $E^{r-1}$   $\gamma' A_1$  l'est aussi. Par une démonstration analogue on montre que si  $\gamma' A_1$  est sous-transitif d'ordre  $(t-1)$  sur  $E^{r-1}$ ,  $(\gamma' A_1) \gamma'^{-1}$  l'est aussi.

Remarque II.1.5.1. : Reprenant les hypothèses du théorème II.1.5, si le sous-groupe normal  $\mathcal{H}_{H'}$  de  $H'$  est lui même sous-transitif d'ordre  $(t-1)$ , alors cela suffit pour que l'on puisse construire  $H$ .

Remarque II.1.5.2. : Si l'on a :  $[H'] = \lambda S^t$ ,  $[G_r] = u S$ , alors  $[\mathcal{H}_{H'}] = \frac{\lambda S^t}{u S} = \frac{\lambda}{u} S^{t-1}$  et  $[A_1] = u \cdot [\mathcal{H}_{H'}] = \lambda S^{t-1}$ .

Si donc on applique tous les éléments de  $H$  ainsi construit à un  $r$ -uplet dont la dernière lettre est  $a_1$ ,  $A_1$  étant sous-transitif d'ordre  $(t-1)$  sur  $E^{r-1}$ , il en résulte que dans le tableau orthogonal obtenu, on obtiendra des  $r$ -uplets dont la dernière composante sera  $a_1$ , les  $(r-1)$  premières constituant un tableau orthogonal  $(\lambda, r-1, S, t-1)$  qui constituera une première transversale du tableau orthogonal  $(\lambda, r-1, S, t)$  engendré par le  $(r-1)$ -uplet déduit du  $r$ -uplet original en supprimant la dernière lettre  $a_1$  et par  $H'$ . Puis de la même façon on obtiendra des  $r$ -uplets dont la dernière lettre sera  $a_2$ , les  $(r-1)$  premières constituant une deuxième transversale disjointe de la précédente etc... Nous remarquons donc la liaison qui existe entre le théorème II.1.5. et le théorème du paragraphe I.9.



Application II.1.5.1. : Nous allons appliquer le théorème II.1.5. et la remarque II.1.5.1. pour démontrer le théorème suivant :

Théorème II.1.5.1. : Quels que soient  $s$  et  $t$ ,  
il existe toujours un tableau orthogonal ( $\lambda = 1$ ,  $r = t+1$ ,  $s$ ,  $t$ )

Démonstration : (Bush avait montré ce théorème pour  $s = p^n$ ,  $p$  étant un nombre premier, grâce à l'utilisation de corps de Galois. L'utilisation des groupes abéliens que nous allons faire per et donc d'obtenir un théorème plus général et montre donc l'intérêt des groupes sous-transitifs).

Soit  $G$  un groupe abélien d'ordre  $s$ . Nous considérons la représentation régulière de  $G$  qui est une représentation transitive. Nous avons donc un groupe de substitutions  $G$  sur un ensemble  $E = G$  avec  $\text{card } E = \text{card } G = s$ .  $G^t$  est évidemment sous-transitif d'ordre  $t$  sur  $E^t$ .

Considérons l'ensemble des éléments  $(e_{i_1}, e_{i_2}, \dots, e_{i_t})$  de  $G^t$  tels que  $e_{i_1} \cdot e_{i_2} \cdot \dots \cdot e_{i_t} = 1$  élément unité de  $G$ .  $G$  étant abélien, cet ensemble forme un sous-groupe normal  $\mathcal{N}_{G^t}$  de  $G^t$ . De plus, pour obtenir un élément de  $\mathcal{N}_{G^t}$ , il suffit de prendre  $(t-1)$  composantes arbitraires, par exemple les  $(t-1)$  premières  $e_{i_1}, e_{i_2}, \dots, e_{i_{t-1}}$  et on a alors  $e_{i_t} = e_{i_1}^{-1} e_{i_2}^{-1} \dots e_{i_{t-1}}^{-1}$ . Ceci entraîne que  $\mathcal{N}_{G^t}$  est d'ordre  $s^{t-1}$ , qu'il est isomorphe à  $G^{t-1}$  et qu'il est sous-transitif d'ordre  $(t-1)$  sur  $E^t$ . Enfin, montrons que nous avons la partition suivante :

$$G^t = \mathcal{N}_{G^t} + \mathcal{N}_{G^t}(1, 1, \dots, 1, e_2) + \dots + \mathcal{N}_{G^t}(1, 1, \dots, 1, e_s)$$

où  $\{1, e_2, \dots, e_s\} = G$ .

En effet, si 2 classes  $\mathcal{N}_{G^t}(1, 1, \dots, 1, e_m)$  et  $\mathcal{N}_{G^t}(1, 1, \dots, 1, e_n)$  étaient identiques on aurait  $i_1, i_2, \dots, i_t$  et  $j_1, j_2, \dots, j_t$  tels que  $(e_{i_1}, e_{i_2}, \dots, e_{i_{t-1}}, e_{i_t} e_m) = (e_{j_1}, e_{j_2}, \dots, e_{j_{t-1}}, e_{j_t} e_n)$

$$\text{Soit } e_{i_k} = e_{j_k} \quad \forall k = 1, 2, \dots, t-1$$



ce qui entraîne  $e_{i_t} = e_{j_t}$  et donc  $e_m = e_n$

Ceci montre que  $G^t/\mathcal{K}_G^t$  est isomorphe à  $G$  groupe de substitutions transitif sur  $E$  et l'on peut donc appliquer le théorème II.1.5 et la remarque qui le suit pour construire un sous-groupe de  $G^{t+1}$  sous-transitif d'ordre  $t$  sur  $E^{t+1}$  et dont l'ordre est égal à celui de  $G^t$ , soit  $s^t$ . Appliquant le théorème II.1.2, l'existence d'un sous-groupe de  $G^{t+1}$  sous-transitif d'ordre  $t$  sur  $E^{t+1}$  entraîne dans ces conditions l'existence d'un tableau orthogonal ( $\lambda = 1, r = t + 1, s, t$ )

Comme il existe des groupes abéliens de tout ordre  $s$ , nous pouvons construire des exemples de tout tableau orthogonal ( $\lambda = 1, r = t + 1, s, t$ ) quels que soient les entiers  $s$  et  $t$ .

Exemple II.1.5.1. : Nous allons illustrer la construction exposée dans la démonstration du théorème précédent, en prenant pour  $G$  le groupe de Klein, groupe de substitutions abélien, transitif sur  $E = \{1, 2, 3, 4\}$  et dont les 4 éléments sont :

$$\pi_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Nous avons alors :

$$\mathcal{K}_G^3 = \left\{ \begin{aligned} &(\pi_0, \pi_0, \pi_0), (\pi_1, \pi_0, \pi_1), (\pi_2, \pi_0, \pi_2), (\pi_3, \pi_0, \pi_3) \\ &(\pi_0, \pi_1, \pi_1), (\pi_1, \pi_1, \pi_0), (\pi_2, \pi_1, \pi_3), (\pi_3, \pi_1, \pi_2) \\ &(\pi_0, \pi_2, \pi_2), (\pi_1, \pi_2, \pi_3), (\pi_2, \pi_2, \pi_0), (\pi_3, \pi_2, \pi_1) \\ &(\pi_0, \pi_3, \pi_3), (\pi_1, \pi_3, \pi_2), (\pi_2, \pi_3, \pi_1), (\pi_3, \pi_3, \pi_0) \end{aligned} \right\}$$

Dans l'isomorphisme  $G^3/\mathcal{K}_G^3 \cong G$







| n° des colonnes | 49 | 59 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |
|-----------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1ère ligne      | 1  | 1  | 1  | 1  | 2  | 2  | 2  | 2  | 3  | 3  | 3  | 3  | 4  | 4  | 4  | 4  |
| 2ème ligne      | 1  | 2  | 3  | 4  | 1  | 2  | 3  | 4  | 1  | 2  | 3  | 4  | 1  | 2  | 3  | 4  |
| 3ème ligne      | 4  | 3  | 2  | 1  | 3  | 4  | 1  | 2  | 2  | 1  | 4  | 3  | 1  | 2  | 3  | 4  |
| 4ème ligne      | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  |

Si l'on considère les éléments de  $E^3$  (1ère ligne, 2ème ligne, 3ème ligne)

les colonnes de 1 à 16 nous donnent une première transversale  
 les colonnes de 17 à 32 nous donnent une deuxième transversale  
 les colonnes de 33 à 48 nous donnent une troisième transversale  
 les colonnes de 49 à 64 nous donnent une quatrième transversale

Ces quatre transversales disjointes de  $E^3$  entraînent évidemment l'existence du tableau orthogonal ( $\lambda = 1$ ,  $r = 4$ ,  $s = 4$ ,  $t = 3$ )  
 On vérifie que chacune de ces transversales constitue bien un tableau orthogonal ( $\lambda = 1$ ,  $r = 3$ ,  $s = 4$ ,  $t = 2$ ).

## II.2 - Les groupes sous-transitifs abéliens d'indice unité : [XII]

Soit  $G_i$  un groupe de substitutions transitif sur un ensemble  $E$  tel que  $\text{card } E = s$ . Comme nous l'avons remarqué dans la démonstration du théorème II.1.5.1, si  $G_i$  est abélien l'ordre de  $G_i$  est égal à  $s$ . Nous allons donc considérer  $r$  groupes  $G_i$

( $i = 1, 2, \dots, r$ ) transitifs sur  $E$  et abéliens et nous remarquons que les propositions (1) et (11) énoncées ci-dessous sont équivalentes :

(1)  $H$  sous groupe de  $\prod_{i=1}^r G_i$  est sous-transitif d'ordre  $t$  sur  $E^r$  et engendre un tableau orthogonal ( $1, r, s, t$ )

(11)  $H$  sous-groupe de  $\prod_{i=1}^r G_i$  est tel que, étant donné n'importe quel élément  $(g_{i_1}, g_{i_2}, \dots, g_{i_t}) \in G_{i_1} \times G_{i_2} \times \dots \times G_{i_t}$  il existe un élément et un seul  $h \in H$  tel que  $g_{i_1}$  soit la composante de  $h$  de rang  $i_1$ ,  $g_{i_2}$  soit la composante de  $h$  de rang  $i_2$ ,  $\dots$ ,  $g_{i_t}$  soit la composante de  $h$  de rang  $i_t$ .



Nous n'utiliserons dans II.2 que (11) ce qui évitera de faire appel à des groupes de substitutions et nous dirons simplement que  $H$  satisfaisant à (11) est sous-transitif d'ordre  $t$  (sans préciser sur quel ensemble) et d'indice unité.

Théorème II.2.1 : Tous sous-groupe  $H$  de  $\prod_{i=1}^r G_i$ , sous-transitif d'ordre  $t < r$  et d'indice unité (les  $G_i$  étant des groupes abéliens d'ordre  $s$ ) peut être considéré comme sous-groupe de  $G^r$ ,  $G$  étant l'un quelconque des  $G_i$ .

Démonstration : Il suffit de montrer que deux quelconques de ces groupes  $G_i$  sont isomorphes. Considérons par exemple  $G_i$  et  $G_j$  ( $i \neq j$ ). Considérons l'ensemble des éléments de  $H$  dont  $(t-1)$  composantes déterminées (et différentes de celles de rang  $i$  et  $j$ ) sont égales à l'unité. Dans cet ensemble, à tout  $g_{i_1} \in G_i$  correspond un et un seul  $g_{j_1} \in G_j$  et réciproquement. La correspondance biunivoque ainsi établie entre éléments de  $G_i$  et éléments de  $G_j$  est un isomorphisme. En effet si l'on considère par exemple les éléments de  $H$  dont les  $(t-1)$  premières composantes sont l'unité et si  $i > t-1$  et  $j > t-1$ , et si

$$(1, 1, \dots, 1, \dots, g_{j_1}, \dots, g_{i_1}, \dots) \in H$$

$$\text{et si } (1, 1, \dots, 1, \dots, g_{j_2}, \dots, g_{i_2}, \dots) \in H$$

$$\text{alors } (1, 1, \dots, 1, \dots, g_{j_1}g_{j_2}, \dots, g_{i_1}g_{i_2}, \dots) \in H$$

Autrement dit l'ensemble des éléments de  $H$  considérés (dont les  $(t-1)$  premières composantes sont l'unité) forme un sous-groupe de  $H$  et cela établit que la correspondance biunivoque envisagée ci-dessus est bien un isomorphisme.

Théorème II.2.2. : Tout sous groupe  $H$  de  $G^r$ , sous-transitif d'ordre  $t < r$  et d'indice unité ( $G$  groupe abélien d'ordre  $s$ ) est de la forme :



$$H = \left\{ (g_{i_1}, g_{i_2}, \dots, g_{i_t}, \prod_{k=1}^{k=t} \sigma_{t+1}^k(g_{i_k}), \dots, \prod_{k=1}^{k=t} \sigma_r^k(g_{i_k}), \forall (g_{i_1}, g_{i_2}, \dots, g_{i_t}) \in G^t \right\}$$

où les  $\sigma_m^n$  ( $m = t+1, t+2, \dots, r$  ;  $n = 1, 2, \dots, t$ ) sont des automorphismes de  $G$ .

Démonstration : En effet considérons le sous-groupe  $H_1$  de  $H$  tel que les  $(t-1)$  composantes consécutives à partir de la 2ème soient égales à l'unité. Nous savons (nous l'avons vu dans la démonstration du théorème précédent) que :

$$H_1 = \left\{ (g_{i_1}, 1, 1, \dots, 1, \sigma_{t+1}^1(g_{i_1}), \dots, \sigma_r^1(g_{i_1}), \forall g_{i_1} \in G \right\}$$

où les  $\sigma_m^1$  sont des bijections de  $G$ . De plus ces bijections de  $G$  conservant les produits, ce sont des automorphismes de  $G$ . Il en va de même pour tous les sous-groupes  $H_j$  de  $H$ ,  $H_j$  étant défini comme le sous-groupe de  $H$  dont les  $t$  premières composantes sont égales à l'unité sauf celle de rang  $j$  ( $j = 1, 2, \dots, t$ ).

$$H_j = \left\{ (1, 1, \dots, 1, g_{i_j}, 1, \dots, 1, \sigma_{t+1}^j(g_{i_j}), \dots, \sigma_r^j(g_{i_j}), \forall g_{i_j} \in G \right\}$$

les  $\sigma_m^j$  étant des automorphismes de  $G$ .

Enfin, tous les  $H_j$  ( $j = 1, 2, \dots, t$ ) étant des sous-groupes abéliens donc sous-groupes normaux de  $H$ , qui n'ont en commun que l'élément unité de  $H$  (en vertu de la sous-transitivité d'ordre  $t$ ) le produit direct  $H_1 \times H_2 \times \dots \times H_t$  est un sous-groupe de  $H$ .

L'ordre de  $\prod_{j=1}^t H_j$  étant  $s^t$ , donc égal à celui de  $H$ , le

produit direct  $\prod_{j=1}^t H_j$  est identique à  $H$  et on a bien démontré le résultat du théorème II.2.2.

Définition II.2.1. : Etant donné un groupe abélien  $G$ , un automorphisme  $A$  de  $G$  sera appelé automorphisme propre de  $G$  si l'équation  $x^{-1} A(x) = u$  admet une solution unique  $x$  dans  $G$ , quelque soit  $u \in G$ . Nous noterons  $\{A\}_G$  l'ensemble des automorphismes propres de  $G$ .



Remarque II.2.1.1. : Si  $A$  est un automorphisme propre du groupe abélien  $G$ , l'opération qui à  $x \in G$  fait correspondre  $x^{-1}A(x) \in G$  est un automorphisme de  $G$ .

Nous noterons  $\hat{A}$  cet automorphisme.

Remarque II.2.1.2. : Si  $A$  est un automorphisme propre du groupe abélien  $G$ ,  $A^{-1}$  est aussi un automorphisme propre de  $G$ .

Remarque II.2.1.3. :  $\left\{ \hat{A}_j J, \forall A_j \in \{A\}_G \right\} = \{A\}_G$

où  $J$  est l'automorphisme qui consiste à inverser chaque élément du groupe abélien  $G$ .

En effet  $\hat{A}_j J(x) = x^{-1} \hat{A}_j(x^{-1}) = x^{-1} x A_j(x^{-1}) = A_j J(x)$

$A_j J$  étant un automorphisme l'équation  $\hat{A}_j J(x) = u$  a bien une solution unique en  $x$ ,  $\forall u \in G$ . On déduit du fait que

$\hat{A}_j J = A_j J$ , que si la correspondance qui fait correspondre à  $A_i$ ,  $\hat{A}_i$  est désignée par  $\Lambda$ , et si la correspondance qui fait correspondre à  $A_i$ ,  $A_i J$  est désignée par  $J^*$ , que l'on a :

$(J^* \Lambda)^2 = I$  application identique. C'est-à-dire que la bijection  $J^* \Lambda$  de  $\{A\}_G$  sur  $\{A\}_G$  admet la même application  $J^* \Lambda$  comme application réciproque.

Remarque II.2.1.4. : Si  $\sigma$  et  $\tau$  sont des automorphismes du groupe abélien  $G$ , tels que  $\sigma \cdot \tau \in \{A\}_G$ , alors  $\tau \sigma \in \{A\}_G$ .  $\{A\}_G$  est une partie distinguée de  $\mathcal{A}(G)$  groupe des automorphismes de  $G$ .

En effet si  $\widehat{\sigma \tau}(x) = u$  admet une solution unique en  $x$  quel que soit  $u \in G$ , il en est de même de  $\widehat{\tau \sigma \tau}(x) = u$

Or  $\widehat{\tau \sigma \tau}(x) = \tau(x^{-1}) \tau \sigma \tau(x) = \widehat{\tau \sigma \tau}(x)$

Or si  $\widehat{\tau \sigma \tau}(x) = u$  admet une solution unique en  $x$ ,  $\forall u$ , elle admet aussi une solution unique en  $\tau(x)$ ,  $\forall u$ .

Il en résulte que  $\tau \sigma$  est bien un automorphisme propre de  $G$ .

Donc si  $\rho \in \{A\}_G$   $\rho = \sigma(\sigma^{-1} \rho) \forall \sigma \in \mathcal{A}(G)$



et d'après ce qui précède  $\sigma^{-1} \rho \sigma \in \{A_G\}, \forall \sigma \in \mathcal{A}(G)$   
 ce qui montre que  $\{A\}_G$  est bien une partie distinguée de  $\mathcal{A}(G)^*$ .

Théorème II.2.3. : Le système  $\prod_{j=1}^2 \sigma_i^j(x_j) = u_i \quad (i = 1, 2)$

où les  $\sigma_i^j$  sont des automorphismes du groupe abélien  $G$  a une solution unique en  $(x_1, x_2) \in G^2$ , quel que soit  $(u_1, u_2) \in G^2$  si et seulement si  $\sigma_1^1(\sigma_2^1)^{-1} \sigma_2^2(\sigma_1^2)^{-1}$  est un automorphisme propre de  $G$ .

Démonstration : En effet, le système est équivalent au système suivant :

$$\begin{cases} X_1 \cdot X_2 = u_1 \\ \left[ \sigma_2^1(\sigma_1^1)^{-1} \right] (X_1) \cdot \left[ \sigma_2^2(\sigma_1^2)^{-1} \right] (X_2) = u_2 \end{cases}$$

qui est équivalent au système :

$$\begin{cases} X_1 \cdot X_2 = u_1 \\ X_1 \cdot \left[ \sigma_1^1(\sigma_2^1)^{-1} \sigma_2^2(\sigma_1^2)^{-1} \right] (X_2) = \left[ \sigma_1^1(\sigma_2^1)^{-1} \right] (u_2) \end{cases}$$

donc

$X_2^{-1} \left[ \sigma_1^1(\sigma_2^1)^{-1} \sigma_2^2(\sigma_1^2)^{-1} \right] (X_2) = v$  a une solution unique en  $X_2, \forall v$

donc  $\sigma_1^1(\sigma_2^1)^{-1} \sigma_2^2(\sigma_1^2)^{-1}$  doit être un automorphisme propre de  $G$ .

$X_2$  étant alors déterminé de façon unique,  $X_1$  est déterminé de façon unique par  $X_1 \cdot X_2 = u_1$ . La condition est donc suffisante.

Définition II.2.2. : Etant donnée une matrice  $(\sigma_i^j)$  à 2 lignes

$(i = 1, 2)$  et à 2 colonnes  $(j = 1, 2)$ , dont les éléments sont des automorphismes d'un groupe abélien fini  $G$ , nous appellerons automorphisme résultant de la matrice  $(\sigma_i^j)$  l'expression

$$\sigma_1^1(\sigma_2^1)^{-1} \sigma_2^2(\sigma_1^2)^{-1}.$$



Remarque II.2.2.1 : Si on permute les 2 lignes de la matrice  $(\sigma_i^j)$ , le résultant de la nouvelle matrice est  $\sigma_2^1(\sigma_1^1)^{-1}\sigma_1^2(\sigma_2^2)^{-1}$  et provient donc de l'ancien par

1) passage à l'inverse :  $\sigma_1^2(\sigma_2^2)^{-1}\sigma_2^1(\sigma_1^1)^{-1}$  et

2) par conjugaison :  $[\sigma_1^2(\sigma_2^2)^{-1}]\sigma_2^1(\sigma_1^1)^{-1}\sigma_1^2(\sigma_2^2)^{-1}[\sigma_1^2(\sigma_2^2)^{-1}]^{-1}$

et donc si le résultant de la 1ère matrice appartient à  $\{A\}_G$ , celui de la 2ème appartient aussi à  $\{A\}_G$ . De la même façon, on montre que si l'on permute 2 colonnes, on obtient une matrice dont le résultant est l'inverse de la matrice initiale et donc si le résultant de la 1ère matrice appartient à  $\{A\}_G$ , celui de la 2ème appartient aussi à  $\{A\}_G$ .

Définition II.2.3. : Soit  $(\sigma_i^j)$  une matrice carrée d'ordre  $n$  dont les éléments  $\sigma_i^j$  sont des automorphismes d'un groupe abélien  $G$ . Supposons que nous ayons défini l'automorphisme résultant de toute matrice carrée d'ordre  $\leq n-1$  (et différent de 1) et que tout automorphisme résultant de toute matrice carrée d'ordre  $\leq n-1$  extraite de  $(\sigma_i^j)$  soit un automorphisme propre de  $G$ . Alors nous définissons l'automorphisme résultant de  $(\sigma_i^j)$  comme l'automorphisme résultant de la matrice carrée d'ordre 2  $(\hat{R}_1^c)$  ( $1 = n, n-1$  ;  $c = n, n-1$ ), où  $R_1^c$  est l'automorphisme résultant de la matrice carrée d'ordre  $(n-1)$  déduite de  $(\sigma_i^j)$  en supprimant de  $(\sigma_i^j)$  la ligne 1 et la colonne  $c$ .

On remarque que si toute matrice carrée d'ordre 2 dont les éléments sont des automorphismes du groupe abélien  $G$  possède un résultant, il n'en est pas de même pour les matrices carrées d'ordre supérieur à 2, la définition supposant que les résultants des matrices carrées d'ordre  $\leq n$  soient des automorphismes propres de  $G$ .



Théorème II.2.4. : Etant donnée  $(\sigma_i^j)$  ( $i, j = 1, 2, \dots, n$ )  
matrice carrée d'ordre  $n$  dont les éléments  $\sigma_i^j$  sont des automor-  
phismes du groupe abélien fini  $G$ , une condition suffisante pour que  
le système : 
$$\prod_{j=1}^n \sigma_i^j (x_j) = u_i \quad (i = 1, 2, \dots, n)$$

ait une solution unique en  $(x_1, x_2, \dots, x_n) \in G^n$ , quel que soit  
 $(u_1, u_2, \dots, u_n) \in G^n$  est que l'ensemble des automorphismes  
résultants de toute matrice carrée d'ordre  $\leq n$  (et différent de 1)  
soit inclu dans l'ensemble  $\{A\}_G$  (supposé non vide) des automor-  
phismes propres de  $G$ .

Démonstration : La définition d'automorphisme résultant dans  
le cas d'une matrice carrée d'ordre  $n$  équivaut à la résolution  
du système donné par élimination : le fait que les automorphismes  
résultants d'ordre 2 appartiennent à  $\{A\}_G$  permet de passer d'une  
matrice carrée d'ordre  $n$  à une matrice carrée d'ordre  $n-1$  en  
éliminant  $x_1$  ; le fait que les automorphismes résultants d'ordre  
3 appartenant à  $\{A\}_G$  entraîne que les automorphismes résultants  
d'ordre 2 de la matrice d'ordre  $n-1$  précédemment obtenue appar-  
tiennent à  $\{A\}_G$  et permet en éliminant  $x_2$  de passer à une matrice  
carrée d'ordre  $n-2$  et ainsi de suite. On en déduit d'ailleurs que  
l'automorphisme résultant d'une matrice  $M'$  carrée d'ordre  $n$ , obte-  
nue en permutant des lignes ou des colonnes d'une matrice  $M$  appar-  
tient à  $\{A\}_G$  si celui de  $M$  appartient à  $\{A\}_G$ .

Théorème II.2.5. : Une condition nécessaire et suffisante pour qu'on  
puisse construire un sous-groupe  $H$  de  $G^r$  sous-transitif d'ordre  
 $t < r-1$  et d'indice unité ( $G$  groupe abélien fini) est qu'il existe  
une matrice  $(\sigma_i^j)$  d'automorphismes de  $G$  ( $i=t+1, t+2, \dots, r; j=1, 2, \dots, t$ )  
de  $(r-t)$  lignes et  $t$  colonnes telle que l'automorphisme résultant  
de toute matrice carrée d'ordre  $n$ , quelque soit  $n \in \{2, 3, \dots, \min(t, r-t)\}$ ,  
extraite de  $(\sigma_i^j)$ , existe et soit un automorphisme propre de  $G$ .



Démonstration : Le théorème II.2.2. montre que

$$H = \left\{ (g_{i_1}, g_{i_2}, \dots, g_{i_t}, \prod_{k=1}^t \sigma_{t+1}^k(g_{i_k}), \dots, \prod_{k=1}^t \sigma_r^k(g_{i_k})), \forall (g_{i_1}, g_{i_2}, \dots, g_{i_t}) \in G^t \right\}$$

Pour que  $H$  soit sous-transitif d'ordre  $t$  et d'indice unité il faut et il suffit que le système

$$\left\{ \begin{array}{l} g_{i_{m_1}} = u_{m_1} \\ g_{i_{m_2}} = u_{m_2} \\ \vdots \\ g_{i_{m_p}} = u_{m_p} \\ \prod_{k=1}^t \sigma_{m_{p+1}}^k(g_{i_k}) = u_{m_{p+1}} \\ \prod_{k=1}^t \sigma_{m_{p+2}}^k(g_{i_k}) = u_{m_{p+2}} \\ \vdots \\ \prod_{k=1}^t \sigma_{m_t}^k(g_{i_k}) = u_{m_t} \end{array} \right.$$

ait une solution unique en  $(g_{i_1}, g_{i_2}, \dots, g_{i_t})$

$$\forall (u_{m_1}, u_{m_2}, \dots, u_{m_t}) \in G^t$$

$$\forall p = 0, 1, 2, \dots, t \text{ si } r - t \geq t$$

$$\forall p = 2t - r, 2t - r + 1, \dots, t \text{ si } r - t < t$$

$$\text{où } \{m_1, m_2, \dots, m_p\} \subseteq \{1, 2, \dots, t\}$$

$$\text{et où } \{m_{p+1}, m_{p+2}, \dots, m_t\} \subseteq \{t+1, t+2, \dots, r\}$$

$$\text{Soit } \{p_1, p_2, \dots, p_{t-p}\} = \begin{cases} \{m_1, m_2, \dots, m_p\} \\ \{1, 2, \dots, t\} \end{cases}$$



Le système précédent équivaut au système :

$$\left\{ \begin{array}{l} \prod_{k=1}^{t-p} \sigma_{m_{p+1}}^{\mu_k} (g_{i \mu_k}) = v_{m_{p+1}} \\ \prod_{k=1}^{t-p} \sigma_{m_{p+2}}^{\mu_k} (g_{i \mu_k}) = v_{m_{p+2}} \\ \vdots \\ \prod_{k=1}^{t-p} \sigma_{m_t}^{\mu_k} (g_{i \mu_k}) = v_{m_t} \end{array} \right.$$

Il faut et il suffit que ce système ait une solution unique en

$$(g_{i \mu_1}, g_{i \mu_2}, \dots, g_{i \mu_{t-p}}), \forall (v_{m_{p+1}}, v_{m_{p+2}}, \dots, v_{m_t}) \in G^{t-p}.$$

Il suffit alors que le résultant de la matrice carrée d'ordre  $t-p$  d'automorphismes de  $G$  appartienne à  $\{A\}_G$  et ceci  $\forall p$  qui prend les valeurs  $t-2, t-3, \dots, 0$  ou  $2t-r$  selon les cas (les cas  $t$  et  $t-1$  étant évidents). Or la condition est nécessaire et suffisante pour les matrices carrées d'ordre 2. Mais si les résultants de toute matrice carrée d'ordre 2 extraites de  $(\sigma_i^j)$  appartiennent à  $\{A\}_G$  un système d'ordre 3 pourra être réduit à un système d'ordre 2 d'où l'on pourra déduire des équations telles que

$$x^{-1} \left( \begin{array}{l} \text{(Résultant d'une matrice carrée)} \\ \text{(d'ordre 3)} \end{array} \right) (x) = u$$

qui doivent avoir une solution unique en  $x$ . La condition est dès lors aussi nécessaire pour les matrices d'ordre 3 et ainsi de suite.

#### Applications du Théorème II.2.5 :

1ère application : Pour que l'on puisse construire un sous-groupe  $H$  de  $G^{t+2}$  ( $G$  groupe abélien fini) sous-transitif d'ordre  $t$  et d'indice unité, il faut et il suffit qu'il existe  $(t-1)$



automorphismes de  $G$   $\{\sigma_i\}_{i=1,2,\dots,t}$  qui soient des automorphismes propres de  $G$  et tels que  $\sigma_i^{-1} \sigma_j$  soit un automorphisme propre de  $G$ ,  $\forall (i, j) (i \neq j)$ .

En effet, la matrice d'automorphismes de  $G$  à 2 lignes et  $t$  colonnes suivante ( $I$  = application identique de  $G$  sur  $G$ ) satisfait alors aux conditions du théorème II.2.5 :

$$\begin{pmatrix} I & I & I & \dots & I \\ I & \sigma_2 & \sigma_3 & \dots & \sigma_t \end{pmatrix}$$

Réciproquement s'il existe une matrice d'automorphismes de  $G$   $(\sigma_i^j)$  à 2 lignes et  $t$  colonnes ( $i = 1, 2 ; j = 1, 2, \dots, t$ ), les conditions sur les résultants d'ordre 2 seront :

$$1) \sigma_1^1 (\sigma_2^1)^{-1} \sigma_2^j (\sigma_1^j)^{-1} = \sigma_j \text{ est un automorphisme propre de } G (j \neq 1)$$

$$(2) \sigma_1^i (\sigma_2^i)^{-1} \sigma_2^j (\sigma_1^j)^{-1} = \sigma_i^{-1} \sigma_j \text{ est un automorphisme propre de } G, (i \neq j)$$

Ce qui montre que cela revient à supposer l'existence des  $t-1$  automorphismes  $\{\sigma_i\}$

2ème application : S'il existe un sous-groupe  $H_1$  de  $G^{t+2}$  ( $G$  groupe abélien fini) sous-transitif d'ordre 2 et d'indice unité, alors il existe un sous-groupe  $H_2$  de  $G^{t+2}$  sous-transitif d'ordre  $t$  et d'indice unité et réciproquement.

En effet l'existence de  $H_1$  équivaut à l'existence d'une matrice d'automorphismes de  $G$  à  $t$  lignes et 2 colonnes  $(\sigma_i^j)$  ( $i = 3, 4, \dots, t+2 ; j = 1, 2$ ) telle que tous les résultants d'ordre 2 soient des automorphismes propres de  $G$  c'est-à-dire que



$$\sigma_{i_1}^1 (\sigma_{i_2}^1)^{-1} \sigma_{i_2}^2 (\sigma_{i_1}^2)^{-1} \in \{A\}_G$$

Considérons alors la matrice  $(\tau_k^1) (k = t+1, t+2; 1 = 1, 2, \dots, t)$

à 2 lignes et t colonnes où  $\tau_k^1 = (\sigma_{1+t}^{k-t})^{-1}$

ou alors  $\tau_{t+1}^{i_1-2} (\tau_{t+2}^{i_1-2})^{-1} \tau_{t+2}^{i_2-2} (\tau_{t+1}^{i_2-2})^{-1} = (\sigma_{i_1}^1)^{-1} \sigma_{i_1}^2 (\sigma_{i_2}^2)^{-1} \sigma_{i_2}^1$

$$= [(\sigma_{i_2}^1)^{-1} \sigma_{i_2}^2 (\sigma_{i_1}^2)^{-1} \sigma_{i_1}^1]^{-1} = (\sigma_{i_1}^1)^{-1} [\sigma_{i_1}^1 (\sigma_{i_2}^1)^{-1} \sigma_{i_2}^2 (\sigma_{i_1}^2)^{-1}]^{-1} \sigma_{i_1}^1$$

qui résulte de  $\sigma_{i_1}^1 (\sigma_{i_2}^1)^{-1} \sigma_{i_2}^2 (\sigma_{i_1}^2)^{-1}$  par inversion et par conjugaison donc qui appartient aussi à  $\{A\}_G$

Ceci démontre donc l'existence du sous-groupe  $H_2$  de  $G^{t+2}$ .

Réciproquement si  $H_2$  existe, c'est que  $(\tau_k^1)$  existe et satisfait

aux conditions du théorème II.2.5. et on montre qu'alors la matrice  $(\sigma_i^j)$  où  $\sigma_i^j = (\tau_{j+t}^{i-2})^{-1}$  satisfait aux conditions du théorème II.2.5. et donc que  $H_1$  existe.

### Conséquence de la 2ème application :

Théorème II.2.5.1 : Etant donné G groupe abélien d'ordre s, il n'existe pas de sous-groupe H de  $G^{t+2}$  sous-transitif d'ordre t et d'indice unité si  $t \geq s$ .

Démonstration : On sait que l'existence de  $H_1$  sous-groupe de  $G^{t+2}$  sous-transitif d'ordre 2 et d'indice unité entraîne celle d'un tableau orthogonal  $(\lambda = 1, t+2, s, t)$  qui équivaut à celle de t quasi-groupes mutuellement orthogonaux d'ordre s (I.5). Or il n'existe pas n quasi-groupes mutuellement orthogonaux pour  $n \geq s$ , ce qui entraîne qu'il n'existe pas de sous-groupe  $H_1$  de  $G^{t+2}$  sous-transitif d'ordre 2 d'indice unité pour  $t \geq s$ , ce qui d'après la 2ème application du théorème II.2.5, équivaut à la non-existence d'un sous-groupe H de  $G^{t+2}$  sous-transitif d'ordre t et d'indice



unité pour  $t \geq s$  et démontre donc le théorème II.2.5.1

### Exemples :

1) le groupe abélien produit direct des 2 groupes cycliques d'ordre 2, soit  $\{2\} \cdot \{2\}$  possède 2 automorphismes propres  $A_1$  et  $A_2$  et  $\{A_1, A_2, I\}$  forme un groupe. Soient  $a$  et  $b$  2 générateurs indépendants du groupe abélien  $\{2\} \cdot \{2\}$ , on a :

$$A_1 = \begin{pmatrix} a & b \\ b & ab \end{pmatrix} \quad A_2 = \begin{pmatrix} a & b \\ ab & a \end{pmatrix}$$

$$A_1 A_2 = I \quad A_1 A_2^{-1} = A_2 \quad A_2 A_1^{-1} = A_1$$

On peut donc en utilisant les 1ère et 2ème applications construire un sous-groupe de  $G^5$  sous-transitif d'ordre 3 et d'indice unité ou un sous-groupe de  $G^5$  sous-transitif d'ordre 2 et d'indice unité qui donneront naissance respectivement à des tableaux orthogonaux  $(1, 5, 4, 3)$  et  $(1, 5, 4, 2)$

2) le groupe abélien produit direct de 3 groupes cycliques d'ordre 2, soit  $\{2\} \cdot \{2\} \cdot \{2\}$  possède 8 ensembles de 6 automorphismes propres, chacun de ces ensembles, étant tel que lorsqu'on y ajoute  $I$  il forme un groupe. Soient  $a, b, c$  3 générateurs indépendants du groupe  $G = \{2\} \cdot \{2\} \cdot \{2\}$ , on a

$$A_1 = \begin{pmatrix} a & b & c \\ ab & bc & a \end{pmatrix} \quad A_2 = \begin{pmatrix} a & b & c \\ ac & abc & ab \end{pmatrix}$$

$$A_3 = \begin{pmatrix} a & b & c \\ b & c & ac \end{pmatrix} \quad A_4 = \begin{pmatrix} a & b & c \\ bc & a & b \end{pmatrix}$$

$$A_5 = \begin{pmatrix} a & b & c \\ abc & ab & bc \end{pmatrix} \quad A_6 = \begin{pmatrix} a & b & c \\ c & ac & abc \end{pmatrix}$$



$\{A_1, A_2, A_3, A_4, A_5, A_6, I\}$  forme un groupe cyclique d'ordre 7. de plus  $\hat{A}_1 = A_3$ ,  $\hat{A}_2 = A_6$ ,  $\hat{A}_3 = A_1$ ,  $\hat{A}_4 = A_5$ ,  $\hat{A}_5 = A_4$  et  $\hat{A}_6 = A_2$ .

En vertu des 1ère et 2ème applications on peut construire un sous-groupe de  $G^9$  sous-transitif d'ordre 7 et d'indice unité et un sous-groupe de  $G^9$  sous-transitif d'ordre 2 et d'indice unité qui donneront naissance respectivement à des tableaux orthogonaux  $(1, 9, 8, 7)$  et  $(1, 9, 8, 2)$ .

3ème application : S'il existe 2 automorphismes propres  $\sigma_1$  et  $\sigma_2$  d'un groupe abélien fini  $G$  d'ordre  $s$ , tels que  $\sigma_1^{-1} \sigma_2$  soit un automorphisme propre de  $G$ , et si l'opération qui à  $x \in G$  associe  $x^{-1} \sigma_i(x^2)$  est un automorphisme de  $G$ ,  $\forall i = 1, 2$ , alors on peut construire un sous-groupe  $H$  de  $G^6$  sous-transitif d'ordre 3, et d'indice unité.

En effet considérons la matrice d'automorphismes de  $G$  à 3 lignes et 3 colonnes ( $J(x) = x^{-1}$ ,  $\forall x \in G$ ) :

$$\begin{pmatrix} I & I & I \\ I & \sigma_1 & \hat{\sigma}_1 J \\ I & \sigma_2 & \hat{\sigma}_2 J \end{pmatrix}$$

Pour qu'elle satisfasse aux conditions du théorème II.2.5, il faut et il suffit que :

1) les automorphismes résultants d'ordre 2 soient des automorphismes propres de  $G$ , soit :

a)  $\sigma_i$  automorphisme propre de  $G$ ,  $\forall i = 1, 2$  ce qui est vrai par hypothèse

b)  $\sigma_1^{-1} \sigma_2$  et  $\sigma_2^{-1} \sigma_1$  automorphismes propres de  $G$  :

$\sigma_1^{-1} \sigma_2$  l'est par hypothèse,  $\sigma_2^{-1} \sigma_1 = (\sigma_1^{-1} \sigma_2)^{-1}$  l'est aussi



c)  $\widehat{\sigma}_1^J$  automorphisme propre de  $G$  : or,

$x^{-1} \widehat{\sigma}_1^J(x) = \sigma_1^J(x)$  automorphisme de  $G$ , donc la condition est réalisée

d)  $\sigma_1^{-1} \widehat{\sigma}_1^J$  automorphisme propre de  $G$  ; or,

$x^{-1}(\sigma_1^{-1} \widehat{\sigma}_1^J)(x) = \sigma_1^J(x^{-1} \sigma_1(x^2))$  et comme on a supposé que l'opération  $x \rightarrow x^{-1} \sigma_1(x^2)$  est un automorphisme, la condition est réalisée.

e)  $\sigma_1 (\sigma_2)^{-1} \widehat{\sigma}_2 (\widehat{\sigma}_1)^{-1}$  automorphisme propre de  $G$  ou encore  $(\widehat{\sigma}_1)^{-1} \sigma_1 (\sigma_2)^{-1} \widehat{\sigma}_2$  automorphisme propre de  $G$ , or

$x^{-1}[(\widehat{\sigma}_1)^{-1} \sigma_1 (\sigma_2)^{-1} \widehat{\sigma}_2](x) = (\widehat{\sigma}_1)^{-1} \widehat{\sigma_1 \sigma_2}^{-1} J(x)$  et la condition est bien réalisée.

2) l'automorphisme résultant d'ordre 3 soit un automorphisme propre de  $G$ . Or il est égal à l'automorphisme résultant d'ordre 2 de la matrice suivante ;

$$\begin{pmatrix} \widehat{\sigma}_1 & \widehat{\sigma_1 J} \\ \widehat{\sigma}_2 & \widehat{\sigma_2 J} \end{pmatrix} = \begin{pmatrix} \widehat{\sigma}_1 & \sigma_1 J \\ \widehat{\sigma}_2 & \sigma_2 J \end{pmatrix}$$

dont le résultant est bien un automorphisme propre de  $G$  en vertu du 1) e).

### Exemples :

1°) Reprenons  $G = \{2\} \{2\}$  produit direct de 2 groupes cycliques d'ordre 2. Les conditions de la 3ème application sont remplies lorsque l'on prend

$$\sigma_1 = \begin{pmatrix} a & b \\ b & ab \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} a & b \\ ab & a \end{pmatrix}$$



(a et b générateurs indépendants de G) et on a bien 2 automorphismes propres  $\sigma_1$  et  $\sigma_2$  tels que  $\sigma_1^{-1} \sigma_2 = \sigma_1$  et de plus tout élément de G étant d'ordre 2, l'opération qui à x associe  $x^{-1} \sigma_i(x^2) = x^{-1}$  n'est autre que l'automorphisme qui consiste à inverser tout élément de G. On peut donc construire un sous-groupe H de  $G^6$  sous-transitif d'ordre 3 et d'indice unité qui donnera naissance à un tableau orthogonal (1, 6, 4, 3).

2°) Reprenons  $G = \{2\} \{2\} \{2\}$

Prenons

$$\sigma_1 = \begin{pmatrix} a & b & c \\ ab & bc & a \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} a & b & c \\ ac & abc & ab \end{pmatrix}$$

On a alors

$$\hat{\sigma}_1 = \begin{pmatrix} a & b & c \\ b & c & ac \end{pmatrix} \quad \hat{\sigma}_2 = \begin{pmatrix} a & b & c \\ c & ac & abc \end{pmatrix}$$

(Ici  $J = I$  puisque tout élément de G est d'ordre 2)

La condition  $x^{-1} \sigma_i(x^2) = \text{automorphisme de G}$  est réalisée puisque  $x^{-1} \sigma_i(x^2) = x^{-1} = x$ . Nous sommes bien dans les conditions de la 3ème application et l'on peut donc construire un sous-groupe H de  $G^6$  sous-transitif d'ordre 3 et d'indice unité qui donnera naissance à un tableau orthogonal (1, 6, 8, 3).

Remarques sur les possibilités de construction de tableaux orthogonaux lorsque les conditions du Théorème II.2.5. sont en défaut :

1°) Supposons que pour le groupe G fini abélien considéré, il n'existe pas d'automorphisme propre. Le théorème II.2.5 permet d'affirmer qu'il n'existe pas de sous-groupe H de  $G^{t+2}$ , sous transitif d'ordre t et d'indice unité.



Soit alors  $\theta$  un automorphisme de  $G$  et soit  $\theta *$  l'opération qui à tout  $x \in G$  fait correspondre  $\theta *(x) = x^{-1} \theta(x)$ .  $\theta *$  est un endomorphisme de  $G$ .

Soit  $K = \theta *(G)$  et soit enfin  $G_0 = \{x \in G \mid \theta *(x) = 1\}$

$G/G_0$  est isomorphe à  $K$  et l'ensemble des  $x \in G$  tels que  $\theta *(x) = u$  ( $u$  élément fixé de  $K$ ) est une classe de  $G_0$  dans  $G$ .

Nous avons donc  $G = G_0 + G_0 x_2 + \dots + G_0 x_n$  ( $[K] = n$ ).

Examinons le cas  $t = 2$ .

Un sous-groupe  $H^{(1)}$  de  $G^4$ , sous-transitif d'ordre 2, d'indice unité et abélien serait de la forme :

$$H^{(1)} = \left\{ (g_{i_1}, g_{i_2}, g_{i_1} g_{i_2}, g_{i_1} \theta(g_{i_2})) \mid (g_{i_1}, g_{i_2}) \in G^2 \right\}$$

où  $\theta$  serait un automorphisme propre de  $G$ . Or nous avons supposé que  $G$  ne possède pas d'automorphisme propre. Dans ces conditions, les différents systèmes à 2 équations à 2 inconnues suivants sont tels que :

$$(1) \quad \begin{cases} g_{i_1} = u \\ g_{i_2} = v \end{cases} \quad \text{admet une solution unique en } (g_{i_1}, g_{i_2}) \quad \forall (u, v) \in G^2$$

$$(2) \quad \begin{cases} g_{i_1} = u \\ g_{i_1} g_{i_2} = v \end{cases} \quad \begin{array}{l} \text{admet une solution unique en } (g_{i_1}, g_{i_2}) \\ \forall (u, v) \in G^2 \end{array}$$

$$(3) \quad \begin{cases} g_{i_1} = u \\ g_{i_1} \theta(g_{i_2}) = v \end{cases} \quad \begin{array}{l} \text{admet une solution unique en } (g_{i_1}, g_{i_2}) \\ \forall (u, v) \in G^2 \end{array}$$

$$(4) \quad \begin{cases} g_{i_2} = u \\ g_{i_1} g_{i_2} = v \end{cases} \quad \begin{array}{l} \text{admet une solution unique en } (g_{i_1}, g_{i_2}) \\ \forall (u, v) \in G^2 \end{array}$$

$$(5) \quad \begin{cases} g_{i_2} = u \\ g_{i_1} \theta(g_{i_2}) = v \end{cases} \quad \begin{array}{l} \text{admet une solution unique en } (g_{i_1}, g_{i_2}) \\ \forall (u, v) \in G^2 \end{array}$$



$$\begin{cases} g_{i_1} g_{i_2} = u \\ g_{i_1} \theta(g_{i_2}) = v \end{cases}$$

admet  $[G_0] = \frac{s}{n} = \lambda$  solutions si  $u^{-1} v \in K$  ( $[G] = s$ )

n'admet aucune solution si  $u^{-1} v \notin K$ .

Donc  $(g_{i_1}, g_{i_2}, g_{i_1} \theta(g_{i_2})) = (u, v)$  intervient  $\lambda$  fois si

$u^{-1} v \in K$  et n'intervient pas si  $u^{-1} v \notin K$ .

Enfin soit  $(1, a_2, a_3, \dots, a_n)$  un système de  $n$  représentants des classes de  $K$  dans  $G$ . Soit  $(\theta a_j)$  la bijection de  $G$  sur lui-même :  $x \rightarrow \theta(a_j x)$ ,  $\forall x \in G$

Nous avons  $(\theta a_j)^* (x) = a_j \theta^* (a_j x)$

lorsque  $x$  balaie  $G$ ,  $\theta^* (a_j x)$  balaie  $K$  et  $a_j \theta^* (a_j x)$  balaie  $a_j K$ . Il en résulte que si nous considérons l'ensemble :

$$H^{(j)} = \left\{ (g_{i_1}, g_{i_2}, g_{i_1} g_{i_2}, g_{i_1} (\theta a_j)(g_{i_2})) \mid \forall (g_{i_1}, g_{i_2}) \in G^2 \right\}$$

les systèmes de 2 équations à 2 inconnues tels que (1), (2), (3), (4), (5) dans lesquels on remplace  $\theta$  par  $\theta a_j$  admettent une solution unique. Quant au système

$$\begin{cases} g_{i_1} g_{i_2} = u \\ g_{i_1} (\theta a_j)(g_{i_2}) = v \end{cases}$$

il équivaut à l'équation  $g_{i_2}^{-1} (\theta a_j)(g_{i_2}) = u^{-1} v$

soit  $(\theta a_j)^* (g_{i_2}) = u^{-1} v$

et admet donc  $\lambda$  solutions si  $u^{-1} v \in a_j K$

et n'admet aucune solution si  $u^{-1} v \notin a_j K$

Il résulte de cela que la réunion disjointe :

$$\bigcup_{j=1}^{j=\lambda} H^{(j)} \text{ forme un tableau orthogonal construit}$$



sur le groupe abélien fini  $G$  d'ordre  $s$ , de 4 lignes, de force 2 et d'indice  $\lambda$ . Enfin :

$$\begin{aligned} & (g_{i_1}, g_{i_2}, g_{i_1}g_{i_2}, g_{i_1}(\theta_{a_j})(g_{i_2})) \cdot (g_{i'_1}, g_{i'_2}, g_{i'_1}g_{i'_2}, g_{i'_1}(\theta_{a_j})(g_{i'_2})) \\ &= (g_{i_1}g_{i'_1}, g_{i_2}g_{i'_2}, g_{i_1}g_{i'_1} \cdot g_{i_2}g_{i'_2}, g_{i_1}g_{i'_1} \theta(a_j g_{i_2}) \theta(a_j g_{i'_2})) \\ & \text{et } \bigcup_{j=1}^{\lambda} H^{(j)} \text{ formera un groupe si et seulement si, } \exists a_k \text{ tel} \end{aligned}$$

$$\text{que : } \theta(a_j g_{i_2}) \theta(a_j g_{i'_2}) = \theta(a_k g_{i_2} g_{i'_2})$$

soit

$$a_j a_{j'} = a_k$$

Donc pour que  $\bigcup_{j=1}^{\lambda} H^{(j)}$  forme un groupe il faut et il suffit qu'il existe un système  $\{1, a_2, a_3, \dots, a_\lambda\}$  de représentants des classes de  $K$  dans  $G$ , qui forment un sous-groupe de  $G$ .

Du point de vue de l'utilisation pratique des tableaux orthogonaux en statistique comme plans d'expériences, on a intérêt à avoir  $\lambda$  le plus faible possible. On utilisera donc de préférence un automorphisme  $\theta$  tel que  $\theta^*(G) = K$  soit le plus grand possible.

Finalement on a le

Théorème II.2.6 : Etant donné  $G$  groupe abélien fini d'ordre  $s$ , si  $\theta$  est un automorphisme de  $G$  tel que  $\theta^*(G) = K$  et que  $[G/K] = \lambda$  on peut construire sur  $G$  un tableau orthogonal  $(\lambda, 4, s, 2)$ .

S'il existe un système de représentants des classes de  $K$  dans  $G$ , formant un groupe, on peut construire un sous-groupe  $H$  de  $G^4$  sous-transitif d'ordre 2 sur  $G^4$ .

2°) Soit  $G$  groupe abélien fini d'ordre  $s$  et considérons l'ensemble :

$$H^{(1)} = \left\{ (g_{i_1}, g_{i_2}, g_{i_3}, g_{i_1}g_{i_2}g_{i_3}, g_{i_1} \theta_2(g_{i_2}) \theta_3(g_{i_3})) , \forall (g_{i_1}, g_{i_2}, g_{i_3}) \in G^3 \right\}$$

dans lequel  $\theta_2$  et  $\theta_3$  sont des automorphismes de  $G$ .



D'après le Théorème II.2.5., pour que  $H^{(1)}$  soit un sous-groupe de  $G^5$  sous-transitif d'ordre 3 d'indice unité, il faut et il suffit que  $\theta_2, \theta_3$  et  $\theta_2^{-1} \theta_3$  soient des automorphismes propres de  $G$ .

a) Supposons que  $\theta_2$  et  $\theta_3$  soient des automorphismes propres de  $G$ , mais que  $\theta_2^{-1} \theta_3$  ne soit pas un automorphisme propre de  $G$  : alors les systèmes :

$$(1) \begin{cases} g_{i_k} = u \\ g_{i_1} = v \\ g_{i_1} g_{i_2} g_{i_3} = w \end{cases} \quad (2) \begin{cases} g_{i_k} = u \\ g_{i_1} = v \\ g_{i_1} \theta_2(g_{i_2}) \theta_3(g_{i_3}) = w \end{cases} \quad (3) \begin{cases} g_{i_m} = u \\ g_{i_1} g_{i_2} g_{i_3} = v \\ g_{i_1} \theta_2(g_{i_2}) \theta_3(g_{i_3}) = w \end{cases}$$

ont une solution unique en  $(g_{i_1}, g_{i_2}, g_{i_3}) \forall (u, v, w) \in G^3$

si  $\{k, l\} \subset \{1, 2, 3\}$  et  $m \in \{2, 3\}$

Quant au système :

$$(4) \begin{cases} g_{i_1} = u \\ g_{i_1} g_{i_2} g_{i_3} = v \\ g_{i_1} \theta_2(g_{i_2}) \theta_3(g_{i_3}) = w \end{cases}$$

il équivaut au système de 2 équations à 2 inconnues :

$$\begin{aligned} g_{i_2} g_{i_3} &= u^{-1} v \\ \theta_2(g_{i_2}) \theta_3(g_{i_3}) &= u^{-1} w \end{aligned}$$

et le nombre de ses solutions est celui de l'équation en  $g_{i_3}$  :

$$g_{i_3}^{-1} (\theta_2^{-1} \theta_3)(g_{i_3}) = v^{-1} u \theta_2^{-1}(u^{-1} w)$$

Soit en reprenant la notation du 1°)

$$(\theta_2^{-1} \theta_3)^*(g_{i_3}) = v^{-1} u \theta_2^{-1}(u^{-1} w)$$

Soit  $K_{2,3} = (\theta_2^{-1} \theta_3)^*(G)$  sous-groupe de  $G$ .



Si  $v^{-1} u \theta_2^{-1}(u^{-1} w) \in K_{2,3}$  l'équation précédente et donc le système (4) aura  $[G]/[K_{2,3}] = \lambda_{2,3}$  solutions.

Si  $v^{-1} u \theta_2^{-1}(u^{-1} w) \notin K_{2,3}$  l'équation précédente et donc le système (4) n'aura aucune solution.

Soit alors  $\{1, a_2, a_3, \dots, a_{\lambda_{2,3}}\}$  un système de représentants des classes de  $K_{2,3}$  dans  $G$ . Considérons alors l'ensemble :

$$H^{(j)} = \left\{ (g_{i_1}, g_{i_2}, g_{i_3}, g_{i_1} g_{i_2} g_{i_3}, g_{i_1} (\theta_2 a_j)(g_{i_2}) \theta_3(g_{i_3})) v(g_{i_1}, g_{i_2}, g_{i_3}) \in G^3 \right\}$$

les systèmes tels que (1), (2), (3) où l'on remplace  $\theta_2$  par  $(\theta_2 a_j)$  ont toujours une solution unique en  $(g_{i_1}, g_{i_2}, g_{i_3})$ , et le système

$$(4)_j \quad \begin{cases} g_{i_1} = u \\ g_{i_1} g_{i_2} g_{i_3} = v \\ g_{i_1} (\theta_2 a_j)(g_{i_2}) \theta_3(g_{i_3}) = w \end{cases}$$

a le même nombre de solutions que l'équation :

$$a_j (\theta_2^{-1} \theta_3)^* (g_{i_3}) = v^{-1} u \theta_2^{-1}(u^{-1} w)$$

qui admet  $\lambda_{2,3}$  solutions si  $v^{-1} u \theta_2^{-1}(u^{-1} w) \in a_j K_{2,3}$

et n'en admet aucune si  $v^{-1} u \theta_2^{-1}(u^{-1} w) \notin a_j K_{2,3}$

Il résulte de cela que la réunion disjointe :

$$\bigcup_{j=1}^{\lambda_{2,3}} H^{(j)} \text{ forme un tableau orthogonal construit sur}$$

le groupe abélien fini  $G$  d'ordre  $s$ , de 5 lignes, de force 3 et d'indice  $\lambda_{2,3}$ . Comme au 1°) on voit que pour que

$\bigcup_{j=1}^{\lambda_{2,3}} H^{(j)}$  forme un groupe il faut et il suffit que l'ensemble  $\{a_j\}_{j=1,2,\dots,\lambda_{2,3}}$  des représentants choisis forme



lui-même un groupe.

Dans le cas particulier où  $\theta_2 = \theta_3$ ,  $K_{2,3} = \{1\}$  et  $\lambda_{2,3} = S$  on obtient un hypercube  $(s, 5, s, 3)$  et  $\{a_j\}$  est  $G$  lui-même donc on obtient un groupe sous-transitif d'ordre 3.

Finalement on a le

Théorème II.2.7 : Etant donné  $G$  groupe abélien fini d'ordre  $s$ , si  $\theta_2$  et  $\theta_3$  sont des automorphismes propres de  $G$  tels que

$(\theta_2^{-1} \theta_3)^*(G) = K$  et que  $[G/K] = \lambda$ , on peut construire sur  $G$  un tableau orthogonal  $(\lambda, 5, s, 3)$ . S'il existe un système de représentants des classes de  $K$  dans  $G$ , formant un groupe, on peut construire un sous-groupe  $H$  de  $G^5$  sous-transitif d'ordre 3 sur  $G^5$ .

b) supposons que  $G$  ne possède pas d'automorphisme propre : alors les systèmes tels que le système (1) ont une solution unique et il en est de même des systèmes tels que le système (2). Par contre un système tel que le système (3), soit par exemple :

$$\left\{ \begin{array}{l} g_{i_2} = u \\ g_{i_1} g_{i_2} g_{i_3} = v \\ g_{i_1} \theta_2(g_{i_2}) \theta_3(g_{i_3}) = w \end{array} \right. \quad \text{a le même nombre de solutions}$$

que l'équation  $\theta_3^*(g_{i_3}) = w v^{-1} u \theta_2(u^{-1})$

qui possède  $\lambda_3 = [G/K_3]$  solutions si  $w v^{-1} u \theta_2(u^{-1}) \in K_3 = \theta_3^*(G)$

et n'en possède aucune si  $w v^{-1} u \theta_2(u^{-1}) \notin K_3$

De la même façon, le système

$$\left\{ \begin{array}{l} g_{i_3} = u \\ g_{i_1} g_{i_2} g_{i_3} = v \\ g_{i_1} \theta_2(g_{i_2}) \theta_3(g_{i_3}) = w \end{array} \right. \quad \text{a le même nombre de}$$



solutions que l'équation  $\theta_2^*(g_{i_2}) = w v^{-1} u \theta_3(u^{-1})$

qui possède  $\lambda_2 = [G/K_2]$  solutions si  $w v^{-1} u \theta_3(u^{-1}) \in K_2 = \theta_2^*(G)$

et n'en possède aucune si  $w v^{-1} u \theta_3(u^{-1}) \notin K_2$ .

Enfin, le système

$$\begin{cases} g_{i_1} = u \\ g_{i_1} g_{i_2} g_{i_3} = v \quad \text{a le même nombre de solutions} \\ g_{i_1} \theta_2(g_{i_2}) \theta_3(g_{i_3}) = w \end{cases}$$

que l'équation

$$(\theta_2^{-1} \theta_3)^*(g_{i_3}) = v^{-1} u \theta_2^{-1}(u^{-1} w)$$

qui possède  $\lambda_{2,3} = [G, K_{2,3}]$  solutions si  $v^{-1} u \theta_2^{-1}(u^{-1} w) \in K_{2,3} = (\theta_2^{-1} \theta_3)^*(G)$

et n'en possède aucune si  $v^{-1} u \theta_2^{-1}(u^{-1} w) \notin K_{2,3}$

Les résultats des théorèmes II.2.6 et II.2.7 nous montrent alors que la juxtaposition des  $\lambda_2 \lambda_3 \lambda_{2,3}$  ensembles :

$$H(j,k,l) = \left\{ (g_{i_1}, g_{i_2}, g_{i_3}, g_{i_1} g_{i_2} g_{i_3}, a_j b_k g_{i_1} \theta_2(c_l g_{i_2}) \cdot \theta_3(g_{i_3})) \right. \\ \left. , \forall (g_{i_1}, g_{i_2}, g_{i_3}) \in G^3 \right\}$$

où

$$\begin{cases} \{1, a_2, a_3, \dots, a_{\lambda_2}\} \\ \{1, b_2, b_3, \dots, b_{\lambda_3}\} \\ \{1, c_2, c_3, \dots, c_{\lambda_{23}}\} \end{cases}$$

sont respectivement des systèmes de représentants des classes de  $K_2$ ,  $K_3$  et  $K_{2,3}$  dans  $G$ , forme un tableau orthogonal construit sur le groupe abélien fini  $\mathbb{Z}$ , de 5 lignes, de force 3, et d'indice

$\lambda = \lambda_1 \lambda_2 \lambda_{23}$ . Nous avons donc le



Théorème II.2.8 : Etant donné  $G$  groupe abélien fini d'ordre  $s$  et 2 automorphismes de  $G$  :  $\theta_2$  et  $\theta_3$  tels que  $\theta_2^*(G) = K_2$ ,

$\theta_3^*(G) = K_3$ ,  $(\theta_2^{-1} \theta_3)^*(G) = K_2 \times K_3$  et  $[G/K_2] = \lambda_2$ ,  $[G/K_3] = \lambda_3$  et  $[G/K_2 \times K_3] = \lambda_2 \lambda_3$ , on peut construire sur  $G$  un tableau orthogonal  $(\lambda = \lambda_2 \lambda_3 \lambda_2 \lambda_3, 5, 8, 3)$

Ce théorème est évidemment susceptible d'être généralisé au cas  $t$  quelconque, mais lorsqu'il n'existe pas d'automorphisme propre de  $G$ , l'indice  $\lambda$  deviendrait si grand que la construction de tels tableaux orthogonaux offrirait peu d'intérêt.

II.3 : Généralisation de la méthode des différences de R.C. BOSE et K.A. BUSH : [X] et [III]

Soit  $G$  un groupe fini d'ordre  $s$ . Considérons  $G^t$  dont les éléments sont  $(g_{i_1}, g_{i_2}, \dots, g_{i_t}) = u_i$ .

$G^t$  admet comme sous-groupe d'ordre  $s$ , l'ensemble des éléments  $(g_1, g_1, \dots, g_1)$  (toutes les composantes sont identiques),  $\forall g_1 \in G$ . Soit  $\mathcal{N}$  ce sous-groupe. L'ensemble des classes à droite de  $\mathcal{N}$  réalise une partition de  $G^t$  en  $s^{t-1}$  classes possédant  $s$  éléments chacune et on peut trouver des éléments  $u_1, u_2, \dots, u_{s^{t-1}}$  de  $G^t$  tels que :

$$G = \mathcal{N}u_1 + \mathcal{N}u_2 + \dots + \mathcal{N}u_{s^{t-1}}$$

Théorème II.3.1 : Soit  $(\alpha_{lc})$  une matrice de  $r$  lignes

( $l = 1, 2, \dots, r$ ) et  $N' = \lambda s^{t-1}$  colonnes ( $c = 1, 2, \dots, N'$ ) dont les éléments appartiennent à  $G$  et qui possède la propriété suivante :

toute sous-matrice de  $t$  lignes et  $N'$  colonnes, extraite de la matrice  $(\alpha_{lc})$  est telle que si l'on considère ses colonnes comme éléments de  $G^t$ , chaque classe  $\mathcal{N}u_k$  soit représentée exactement



$\lambda$  fois.

Alors la méthode de construction d'un tableau orthogonal  $(\lambda, r, s, t)$  est la suivante : remplacer chaque élément  $\alpha_{1c}$  de la matrice précédente par la ligne  $(g_0 \alpha_{1c}, g_1 \alpha_{1c}, \dots, g_{s-1} \alpha_{1c})$   
 $(G = \{g_i, \forall i = 0, 1, 2, \dots, s-1\})$

En effet si l'on prend  $t$  lignes de la matrice ainsi formée, soit les lignes  $l_1, l_2, \dots, l_t$ , l'ensemble des colonnes considérées comme éléments de  $G^t$  est :

$$\{(g_i \alpha_{1_1c}, g_i \alpha_{1_2c}, \dots, g_i \alpha_{1_tc}), \forall c = 1, 2, \dots, \lambda s^{t-1}, \\ \forall i = 0, 1, 2, \dots, s-1\}$$

Or  $\{(g_i \alpha_{1_1c}, g_i \alpha_{1_2c}, \dots, g_i \alpha_{1_tc}), \forall i = 0, 1, 2, \dots, s-1\}$  est identique à la classe  $\mathcal{N}(\alpha_{1_1c}, \alpha_{1_2c}, \dots, \alpha_{1_tc})$  de  $\mathcal{N}$  dans  $G^t$

et donc l'ensemble des colonnes considérées est constitué par l'ensemble des éléments de  $G^t$ , chacun étant répété  $\lambda$  fois. On a donc bien obtenu un tableau orthogonal  $(\lambda, r, s, t)$ .

Dans le cas où  $t = 2$ , nous obtenons une partition de  $G^2$  en  $s$  classes et cette partition peut aussi être obtenue à l'aide de la relation d'équivalence définie par

$$(g_k, g_l) \mathcal{R} (g_m, g_n) \iff g_l^{-1} g_k = g_n^{-1} g_m$$

En utilisant la notation additive on obtient bien la méthode des différences de R.C. Bose et K.A. Bush.

### Applications du Théorème II.3.1 : [XIII]

1ère application : construction de tableaux orthogonaux  
 $(\lambda = h^{t-1}, r, s, t)$  ( $h = \text{nombre entier quelconque}$ ) :

Soit  $K$  un groupe abélien fini d'ordre  $hs$ ,  $H$  un sous-groupe de  $K$ ,  $h$  l'ordre de  $H$  et soit  $G = K/H$ .

Soit  $(a_{1c})$  une matrice de  $r$  lignes et  $(hs)^{t-1}$  colonnes dont les éléments appartiennent à  $K$  et soit  $a_{0c}$  la colonne de rang  $c$  de la matrice  $(a_{1c})$ . Nous définissons  $(a_{1c})$  par :



$$a_{0c} = (k_{i_1} k_{i_2} \dots k_{i_{t-1}}, \tau_1^1(k_{i_1}) \cdot \tau_1^2(k_{i_2}) \dots \tau_1^{t-1}(k_{i_{t-1}}), \tau_2^1(k_{i_1}) \tau_2^2(k_{i_2}) \dots \tau_2^{t-1}(k_{i_{t-1}}), \dots, \tau_{r-1}^1(k_{i_1}) \tau_{r-1}^2(k_{i_2}) \dots \tau_{r-1}^{t-1}(k_{i_{t-1}}))$$

où  $(k_{i_1}, k_{i_2}, \dots, k_{i_{t-1}})$  décrit  $K^{t-1}$  lorsque  $c$  décrit l'ensemble des indices de colonne et où les  $\tau_m^n$  ( $m = 1, 2, \dots, r-1; n = 1, 2, \dots, t-1$ ) sont des automorphismes de  $K$ .

Théorème II.3.2. : une condition suffisante pour qu'on puisse construire à partir de la matrice  $(a_{lc})$  précédente une matrice  $(\alpha_{lc})$  dont les éléments appartiennent à  $G = K/H$  et qui permette la construction d'un tableau orthogonal  $(\lambda = h^{t-1}, r, s, t)$  par l'application du théorème II.3.1 est qu'il existe une matrice  $(\sigma_m^n)$  d'automorphismes de  $K$  ( $m = 1, 2, \dots, r; n = 1, 2, \dots, t$ ;

$\sigma_r^n = \sigma_m^t = I$  application identique de  $K$ ;  $\sigma_m^n = \tau_m^n$  pour  $m \neq r$  et  $n \neq t$ ;  $r > t$ ) telle que le résultant de toute matrice carrée d'ordre  $t$  extraite de  $(\sigma_m^n)$  existe et soit un automorphisme propre de  $K$ .

On a alors  $\alpha_{lc} = \mathcal{H}(a_{lc})$ ,  $\mathcal{H}$  étant l'homomorphisme  $K \rightarrow K/H = G$

En effet, avec la définition que nous avons donnée a priori de  $a_{0c}$ , il faut

a) que l'ensemble des identités :

$$e_a \quad k_{i_1} k_{i_2} \dots k_{i_{t-1}} = k_{j_1} k_{j_2} \dots k_{j_{t-1}} \quad e_a \in K$$

$$e_a \quad \prod_{u=1}^{t-1} \tau_{\mu_1}^u(k_{i_u}) = \prod_{u=1}^{t-1} \tau_{\mu_1}^u(k_{j_u})$$

$$\dots\dots\dots$$

$$e_a \quad \prod_{u=1}^{t-1} \tau_{\mu_{t-1}}^u(k_{i_u}) = \prod_{u=1}^{t-1} \tau_{\mu_{t-1}}^u(k_{j_u})$$







$$e_a = \prod_{u=1}^{t-1} \tau_{j_u}^u (A_{i_u}) = 1 \quad (b = 1, 2, \dots, t)$$

$$A_{i_u} = k_{i_u} k_{j_u}^{-1}$$

admet une solution unique. celle-ci est évidemment  $e_a = 1$  et  $A_{i_u} = 1$ ,  $\forall u = 1, 2, \dots, t-1$ . On a donc bien

$$e_a = 1 \text{ et } k_{i_u} = k_{j_u}, \forall u = 1, 2, \dots, t-1$$

Il en résulte que dans les conditions du Théorème II.3.2, la matrice  $(a_{lc})$  répond aux conditions du théorème II.3.1 et que la matrice  $(\alpha_{lc})$  où  $\alpha_{lc} = \mathcal{K}(a_{lc})$  répond aussi à ses conditions.

Nous allons voir que dans le cas  $t = 2$ , nous pouvons construire aussi des tableaux orthogonaux en utilisant le théorème II.3.1 mais avec des conditions moins restrictives que dans le cas  $t$  quelconque.

2ème application : construction de tableaux orthogonaux  
 $(\lambda, r, s, t=2)$  ( $\lambda$  entier quelconque)

Définition II.3.1 : une bijection  $\theta$  d'un groupe  $K$  sur lui-même est dite orthomorphisme de  $K$  si l'application  $x \rightarrow \theta(x).x^{-1}$ ,  $x \in K$ , est aussi une bijection de  $K$  sur lui-même.

Définition II.3.2 : deux orthomorphismes  $\theta_1$  et  $\theta_2$  d'un groupe  $K$  sont dits orthogonaux si l'application  $x \rightarrow \theta_1(x) [\theta_2(x)]^{-1}$ ,  $x \in K$ , est une bijection de  $K$  sur lui-même.

Soit  $K$  un groupe fini admettant  $H$  comme sous-groupe normal. Soit  $\lambda$  l'ordre de  $K$ ,  $\lambda$  l'ordre du sous-groupe normal de  $H$  et  $G = K/H$ .

Soit  $(a_{lc})$  une matrice de  $(r-1)$  lignes et  $\lambda s$  colonnes dont les éléments appartiennent à  $K$  et soit  $a_{0c}$  la colonne de rang  $c$  de  $(a_{lc})$ . Nous définissons  $(a_{lc})$  par :

$$a_{0c} = (k_i, \sigma_1(k_i), \sigma_2(k_i), \dots, \sigma_{r-2}(k_i))$$



où  $k_i$  décrit  $K$  lorsque  $c$  décrit l'ensemble des indices de colonne et où les  $\sigma_m$  ( $m = 1, 2, \dots, r-2$ ) sont des bijections de  $K$  sur lui-même.

Théorème II.3.3 : Une condition suffisante pour qu'on puisse construire à partir de la matrice  $(a_{lc})$  précédente une matrice  $(\alpha_{lc})$  dont les éléments appartiennent à  $G = K/H$  et qui permette la construction d'un tableau orthogonal  $(\lambda, r, s, 2)$  par l'application du Théorème II.3.1 est qu'il existe des bijections

$\sigma_m$  ( $m = 1, 2, \dots, r-2$ ) qui forment une famille d'orthomorphismes de  $K$  mutuellement orthogonaux. On a alors  $\alpha_{lc} = \mathcal{H}(a_{lc})$ ,

$\mathcal{H}$  étant l'homomorphisme  $K \longrightarrow K/H = G$ .

En effet si on prend un couple de lignes, la  $(m+1)^{\text{ème}}$  et la  $(n+1)^{\text{ème}}$  par exemple,  $\sigma_m(k_i) [\sigma_n(k_i)]^{-1}$  décrit  $K$  lorsque  $k_i$  décrit  $K$  puisque  $\sigma_m$  et  $\sigma_n$  sont des orthomorphismes orthogonaux de  $K$ . Si l'on prend la  $l^{\text{ème}}$  et la  $(m+1)^{\text{ème}}$  lignes,  $k_i [\sigma_m(k_i)]^{-1}$  décrit tout  $K$  puisque  $\sigma_m$  est un orthomorphisme de  $K$ . Or si  $\sigma_m(k_i) \cdot [\sigma_n(k_i)]^{-1}$  décrit tout  $K$  lorsque  $k_i$  décrit  $K$ , l'équation :

$$\mathcal{H} \left[ \sigma_m(k_i) \cdot (\sigma_n(k_i))^{-1} \right] = u, \quad u \in K/H$$

admet exactement  $\lambda$  solutions en  $k_i$ .

$$\text{Or } \mathcal{H} \left[ \sigma_m(k_i) \cdot (\sigma_n(k_i))^{-1} \right] = \mathcal{H} [\sigma_m(k_i)] \cdot (\mathcal{H} [\sigma_n(k_i)])^{-1}$$

la matrice  $(\alpha_{lc})$  permet donc la construction d'un tableau orthogonal  $(\lambda, r-1, s, t=2)$ .

Le  $[(k-1)s + i+1]^{\text{ème}}$  élément de la  $l^{\text{ème}}$  ligne du tableau ainsi formé est :

$$g_i \cdot \alpha_{lk} \quad \left( G = \{g_0, g_1, g_2, \dots, g_{s-1}\} \right)$$



La ligne que nous ajoutons est constituée de la façon suivante :  
le  $[(k-1)s + i + 1]$ ème élément est  $g_j$  si  $j\lambda + 1 \leq k \leq (j+1)\lambda$ .

On vérifie que le tableau de  $r$  lignes formé de cette manière est bien un tableau orthogonal  $(\lambda, r, s, 2)$ .

Exemple : construction de tableaux orthogonaux ( $\lambda = p^u, \lambda s + 1, s = p^v, 2$ ) où  $p$  est un nombre premier

On considère le corps de Galois  $GF(p^{u+v})$  ayant  $p^{u+v}$  éléments. On peut exprimer ses éléments comme des polynômes de degré  $u + v - 1$  dont les coefficients appartiennent à  $GF(p)$  corps des restes des nombres entiers mod  $(p)$ . Nous numérotions les éléments de la façon suivante :

$$\text{si } \alpha_i = \sum_{j=0}^{n-1} a_j x^j, \text{ alors}$$

$i = a_{n-1} a_{n-2} \dots a_1 a_0$  dans le système de numération  $p$ -aire ( $n = u + v$ ). Considérons la sous-classe  $M$  des éléments de  $GF(p^{u+v})$  tels que les coefficients de  $x^v$  et des puissances supérieures de  $x$  sont nuls.  $M$  est constituée des  $p^v$  premiers éléments de  $GF(p^{u+v})$  avec notre système de numération. Établissons alors une correspondance entre les éléments du corps et ceux de  $M$  de la façon suivante : à  $\alpha_i$  de  $GF(p^{u+v})$  correspond l'élément

$$\alpha_k = \sum_{j=0}^{v-1} a_j x^j$$

$\alpha_k$  est déterminé de façon unique par  $\alpha_i$  et  $k = i \bmod (p^v)$ . Réciproquement, à un  $\alpha_k \in M$  correspondent  $p^u$  éléments de

$GF(p^{u+v})$ . Si nous écrivons les lignes de la table de multiplication de  $GF(p^{u+v})$  et que nous remplaçons chaque élément par l'élément qui lui correspond dans  $M$ , nous obtenons une matrice de  $p^{u+v}$  lignes,  $p^{u+v}$  colonnes dont les éléments sont ceux de  $M$  et si nous prenons les différences des éléments correspondants de 2 lignes de la table de multiplication de  $GF(p^{u+v})$  chaque élément



intervient exactement une fois. D'autre part si  $\alpha_i$  et  $\alpha_i$ , correspondent respectivement à  $\alpha_k$  et  $\alpha_k$ , de  $M$ , alors à l'élément  $\alpha_i - \alpha_i$ , de  $GF(p^{u+v})$  correspond l'élément  $\alpha_k - \alpha_k$ , de  $M$  ce qui nous montre que dans la matrice obtenue chaque élément de  $M$  intervient  $p^u$  fois parmi les différences des éléments de 2 lignes correspondantes. Or nous pouvons identifier  $GF(p^{u+v})$  au groupe  $K$  du théorème II.3.3., l'opération de ce groupe étant l'addition, les orthomorphismes mutuellement orthogonaux  $\sigma_m$  étant identifiés avec la multiplication par un élément fixé de  $GF(p^{u+v})$  différent de l'élément 0 (il y en a  $p^{u+v} - 1$ ) le sous groupe  $H$  étant identifié avec l'ensemble des éléments de  $GF(p^{u+v})$  tels que

$$\sum_{j=v}^{u+v} a_j x^j, \text{ et } G = K/H \text{ étant alors isomorphe à } M.$$

On est donc bien dans les conditions d'application du théorème II.3.3. Si on prend  $p = 2$ ,  $u = 1$ ,  $v = 2$ , on opère alors dans  $GF(2^3)$  et on obtient par cette méthode le tableau suivant qui est un tableau orthogonal  $(2, 9, 4, 2)$  :

| des colonnes | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|--------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| 1ère ligne   | 0 | 1 | 2 | 3 | 0 | 1 | 2 | 3 | 0 | 1  | 2  | 3  | 0  | 1  | 2  | 3  |
| 2ème ligne   | 0 | 1 | 2 | 3 | 1 | 0 | 3 | 2 | 2 | 3  | 0  | 1  | 3  | 2  | 1  | 0  |
| 3ème ligne   | 0 | 1 | 2 | 3 | 2 | 3 | 0 | 1 | 0 | 1  | 2  | 3  | 2  | 3  | 0  | 1  |
| 4ème ligne   | 0 | 1 | 2 | 3 | 3 | 2 | 1 | 0 | 2 | 3  | 0  | 1  | 1  | 0  | 3  | 2  |
| 5ème ligne   | 0 | 1 | 2 | 3 | 0 | 1 | 2 | 3 | 1 | 0  | 3  | 2  | 1  | 0  | 3  | 2  |
| 6ème ligne   | 0 | 1 | 2 | 3 | 1 | 0 | 3 | 2 | 3 | 2  | 1  | 0  | 2  | 3  | 0  | 1  |
| 7ème ligne   | 0 | 1 | 2 | 3 | 2 | 3 | 0 | 1 | 1 | 0  | 3  | 2  | 3  | 2  | 1  | 0  |
| 8ème ligne   | 0 | 1 | 2 | 3 | 3 | 2 | 1 | 0 | 3 | 2  | 1  | 0  | 0  | 1  | 2  | 3  |
| 9ème ligne   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1  | 1  | 1  | 1  | 1  | 1  | 1  |



| ° des colonnes | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|----------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1ère ligne     | 0  | 1  | 2  | 3  | 0  | 1  | 2  | 3  | 0  | 1  | 2  | 3  | 0  | 1  | 2  | 3  |
| 2ème ligne     | 0  | 1  | 2  | 3  | 1  | 0  | 3  | 2  | 2  | 3  | 0  | 1  | 3  | 2  | 1  | 0  |
| 3ème ligne     | 1  | 0  | 3  | 2  | 3  | 2  | 1  | 0  | 1  | 0  | 3  | 2  | 3  | 2  | 1  | 0  |
| 4ème ligne     | 1  | 0  | 3  | 2  | 2  | 3  | 0  | 1  | 3  | 2  | 1  | 0  | 0  | 1  | 2  | 3  |
| 5ème ligne     | 3  | 2  | 1  | 0  | 3  | 2  | 1  | 0  | 2  | 3  | 0  | 1  | 2  | 3  | 0  | 1  |
| 6ème ligne     | 3  | 2  | 1  | 0  | 2  | 3  | 0  | 1  | 0  | 1  | 2  | 3  | 1  | 0  | 3  | 2  |
| 7ème ligne     | 2  | 3  | 0  | 1  | 0  | 1  | 2  | 3  | 3  | 2  | 1  | 0  | 1  | 0  | 3  | 2  |
| 8ème ligne     | 2  | 3  | 0  | 1  | 1  | 0  | 3  | 2  | 1  | 0  | 3  | 2  | 2  | 3  | 0  | 1  |
| 9ème ligne     | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 3  | 3  | 3  | 3  | 3  | 3  | 3  | 3  |

#### II.4 : Groupes 2 fois transitifs et tableaux orthogonaux idempotents de force 2 :

Soit  $G$  un groupe fini, 2 fois transitif sur un ensemble  $E$  d'ordre  $s$ . Soit  $E = \{e_1, e_2, \dots, e_s\}$

$G$  étant 2 fois transitif sur  $E$ , son ordre est un multiple de  $s(s-1)$  soit  $\lambda s(s-1)$ .

Soit  $H$  le sous-groupe de  $G^s$  défini par :

$$H = \{(x, x, \dots, x) \mid \forall x \in G\}$$

$H$  est un sous-groupe de  $G^s$  isomorphe à  $G$ .

Il opère sur  $E^s$  en tant que groupe de substitutions.

Juxtaposons les résultats de la transformation de l'élément  $(e_1, e_2, \dots, e_s) \in E^s$  par chacun des éléments de  $H$  (chaque élément de  $E^s$  obtenu étant disposé en colonne).

Nous obtenons un tableau de  $\lambda s(s-1)$  colonnes, soit  $T_1$  ce tableau. Si nous considérons un couple de lignes de ce tableau  $T_1$ , celle qui correspond à l'élément  $e_i$  et celle qui correspond à l'élément



$e_j$  par exemple, nous obtenons  $\lambda s(s-1)$  doublets de la forme  $(x(e_i), x(e_j))$ ,  $\forall x \in G$ . Il en résulte, puisque  $G$  est 2 fois transitif et  $e_i \neq e_j$ , que nous obtenons  $\lambda$  fois tous éléments de  $E^2$  tels que les 2 composantes de chaque élément soient différentes. Juxtaposons alors à côté du tableau  $T_1$ , les  $s$  colonnes  $(e_i, e_i, \dots, e_i)$  de  $E^s$ ,  $\forall e_i \in E$ , et répétons les  $\lambda$  fois chacune, nous obtenons ainsi un tableau  $T$  de  $\lambda s^2$  colonnes. Lorsque nous prenons un couple de lignes, nous obtenons  $\lambda$  fois les couples  $(e_j, e_i)$  ( $j \neq i$ ) provenant de  $T_1$  et  $\lambda$  fois les couples  $(e_i, e_i)$  provenant des colonnes que nous venons de lui adjoindre. On obtient donc  $\lambda$  fois chaque couple  $(e_i, e_j)$  et  $T$  est donc un tableau orthogonal  $(\lambda, s, s, 2)$ . On remarque que ce tableau est idempotent.

Théorème II.4.1 : Etant donné un ensemble  $E$  fini d'ordre  $s$ , s'il existe un groupe 2 fois transitif sur  $E$ ,  $G$ , on peut construire un tableau orthogonal  $(\lambda, s, s, 2)$  idempotent.

$$(\lambda = \frac{\text{ordre de } G}{s(s-1)})$$

Exemple : Le groupe  $G$  engendré par les 3 permutations ( $G$  opère sur l'ensemble des 9 premiers nombres entiers) :

$$A_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 & 9 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 8 & 7 & 4 & 3 & 2 & 1 & 9 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 7 & 3 & 8 & 6 & 5 & 2 & 4 & 1 \end{pmatrix}$$

est un groupe 2 fois transitif sur l'ensemble des 9 premiers nombres entiers, d'ordre  $72 = 9 \times 8$  (sous-groupe du groupe de Mathieu de degré 12).

Par application du Théorème II.4.1, il permet la construction d'un tableau orthogonal  $(1, 9, 9, 2)$  idempotent de 81 colonnes,



c'est-à-dire encore, puisque dans ce cas particulier  $\lambda = 1$ ,  
de 7 quasi-groupes mutuellement orthogonaux idempotents.

Nous exhibons ci-dessous le tableau orthogonal ainsi  
construit.  $T_1$  est constitué des 72 premières colonnes, Le tableau  
tout entier en comprenant 81 :

| des colonnes | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|--------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1ère ligne   | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 3  | 3  | 3  | 3  | 3  | 3  |
| 2ème ligne   | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 1  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 1  | 2  | 4  | 5  | 6  | 7  |
| 3ème ligne   | 3  | 6  | 8  | 7  | 9  | 4  | 5  | 2  | 5  | 4  | 7  | 6  | 8  | 9  | 1  | 3  | 8  | 6  | 1  | 2  | 7  | 5  |
| 4ème ligne   | 4  | 7  | 6  | 2  | 5  | 9  | 3  | 8  | 7  | 1  | 8  | 4  | 3  | 6  | 9  | 5  | 5  | 8  | 2  | 9  | 1  | 4  |
| 5ème ligne   | 5  | 8  | 2  | 6  | 4  | 3  | 9  | 7  | 3  | 6  | 5  | 9  | 7  | 1  | 4  | 8  | 6  | 4  | 7  | 1  | 9  | 8  |
| 6ème ligne   | 6  | 9  | 5  | 4  | 2  | 8  | 7  | 3  | 6  | 7  | 9  | 8  | 1  | 3  | 5  | 4  | 9  | 7  | 8  | 6  | 5  | 2  |
| 7ème ligne   | 7  | 5  | 3  | 9  | 8  | 6  | 2  | 4  | 4  | 8  | 6  | 3  | 9  | 5  | 7  | 1  | 7  | 1  | 5  | 8  | 4  | 9  |
| 8ème ligne   | 8  | 4  | 9  | 3  | 7  | 2  | 6  | 5  | 9  | 5  | 1  | 7  | 4  | 8  | 3  | 6  | 2  | 9  | 6  | 4  | 8  | 1  |
| 9ème ligne   | 9  | 2  | 7  | 8  | 3  | 5  | 4  | 6  | 8  | 9  | 3  | 1  | 5  | 4  | 6  | 7  | 4  | 5  | 9  | 7  | 2  | 6  |
| des colonnes | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 |
| 1ère ligne   | 3  | 3  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 4  | 5  | 5  | 5  | 5  | 5  | 5  | 5  | 5  | 6  | 6  | 6  | 6  |
| 2ème ligne   | 8  | 9  | 1  | 2  | 3  | 5  | 6  | 7  | 8  | 9  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 1  | 2  | 3  |
| 3ème ligne   | 9  | 4  | 2  | 5  | 7  | 9  | 3  | 8  | 6  | 1  | 6  | 8  | 1  | 3  | 4  | 2  | 7  | 8  | 4  | 7  | 9  | 2  |
| 4ème ligne   | 7  | 6  | 3  | 6  | 5  | 8  | 9  | 2  | 1  | 7  | 9  | 3  | 8  | 7  | 2  | 1  | 6  | 4  | 8  | 9  | 4  | 5  |
| 5ème ligne   | 2  | 5  | 8  | 7  | 1  | 3  | 2  | 9  | 5  | 6  | 7  | 6  | 2  | 9  | 8  | 4  | 3  | 1  | 9  | 8  | 7  | 3  |
| 6ème ligne   | 4  | 1  | 5  | 9  | 8  | 1  | 7  | 6  | 3  | 2  | 4  | 8  | 6  | 1  | 3  | 9  | 2  | 7  | 2  | 1  | 5  | 7  |
| 7ème ligne   | 6  | 2  | 6  | 8  | 2  | 7  | 5  | 1  | 9  | 3  | 2  | 4  | 9  | 8  | 7  | 3  | 1  | 6  | 5  | 3  | 1  | 9  |
| 8ème ligne   | 5  | 7  | 7  | 3  | 9  | 6  | 1  | 5  | 2  | 8  | 8  | 1  | 7  | 2  | 9  | 6  | 4  | 3  | 3  | 5  | 2  | 8  |
| 9ème ligne   | 1  | 8  | 9  | 1  | 6  | 2  | 8  | 3  | 7  | 5  | 3  | 7  | 4  | 6  | 1  | 8  | 9  | 2  | 7  | 4  | 8  | 1  |



| des colonnes | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 |
|--------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1ère ligne   | 6  | 6  | 6  | 6  | 7  | 7  | 7  | 7  | 7  | 7  | 7  | 7  | 8  | 8  | 8  | 8  | 8  | 8  | 8  | 8  | 9  | 9  |
| 2ème ligne   | 5  | 7  | 8  | 9  | 1  | 2  | 3  | 4  | 5  | 6  | 8  | 9  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 9  | 1  | 2  |
| 3ème ligne   | 8  | 1  | 3  | 5  | 3  | 1  | 8  | 9  | 4  | 5  | 2  | 6  | 9  | 4  | 2  | 5  | 3  | 1  | 6  | 7  | 7  | 8  |
| 4ème ligne   | 7  | 3  | 2  | 1  | 6  | 5  | 9  | 1  | 3  | 8  | 4  | 2  | 2  | 7  | 6  | 9  | 1  | 4  | 5  | 3  | 4  | 1  |
| 5ème ligne   | 4  | 5  | 1  | 2  | 4  | 9  | 5  | 8  | 2  | 1  | 6  | 3  | 5  | 1  | 9  | 6  | 7  | 3  | 2  | 4  | 2  | 3  |
| 6ème ligne   | 3  | 4  | 9  | 8  | 8  | 3  | 2  | 6  | 9  | 4  | 1  | 5  | 7  | 5  | 4  | 3  | 2  | 9  | 1  | 6  | 3  | 4  |
| 7ème ligne   | 2  | 8  | 4  | 7  | 9  | 6  | 4  | 2  | 1  | 3  | 5  | 8  | 3  | 9  | 7  | 1  | 6  | 2  | 4  | 5  | 8  | 5  |
| 8ème ligne   | 1  | 9  | 7  | 4  | 5  | 4  | 6  | 3  | 8  | 2  | 9  | 1  | 4  | 6  | 1  | 7  | 9  | 5  | 3  | 2  | 6  | 7  |
| 9ème ligne   | 9  | 2  | 5  | 3  | 2  | 8  | 1  | 5  | 6  | 9  | 3  | 4  | 6  | 3  | 5  | 2  | 4  | 7  | 9  | 1  | 5  | 6  |

| des colonnes | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 |
|--------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1ère ligne   | 9  | 9  | 9  | 9  | 9  | 9  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 2ème ligne   | 3  | 4  | 5  | 6  | 7  | 8  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 3ème ligne   | 5  | 6  | 1  | 2  | 3  | 4  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 4ème ligne   | 2  | 3  | 6  | 7  | 8  | 5  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 5ème ligne   | 4  | 1  | 8  | 5  | 6  | 7  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 6ème ligne   | 1  | 2  | 7  | 8  | 5  | 6  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 7ème ligne   | 6  | 7  | 4  | 1  | 2  | 3  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 8ème ligne   | 8  | 5  | 2  | 3  | 4  | 1  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |
| 9ème ligne   | 7  | 8  | 3  | 4  | 1  | 2  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  |



II.5 : Deux méthodes de construction de tableaux orthogonaux à partir de corps de Galois :

II.5.1 : Construction de tableaux orthogonaux  $(1, s+1, s=p^n, t < s)$  (p étant un nombre premier) : [V]

Théorème II.5.1 : Si  $s = p^n$ , où  $p$  est un nombre premier et  $s > t$ , alors on peut construire des tableaux orthogonaux  $(1, s+1, s, t)$ .

Démonstration : Soit  $GF(s)$  le corps de Galois ayant  $s = p^n$  éléments

$e_0, e_1, e_2, \dots, e_{s-1}$ . Considérons les polynômes :

$$y_j(x) = \sum_{i=0}^{t-1} a_i x^i \text{ où les coefficients } a_i \text{ appartiennent}$$

à  $GF(s)$ . Il existe  $s^t$  tels polynômes et donc l'indice  $j$  prend ses valeurs dans l'ensemble :  $\{0, 1, 2, \dots, j, \dots, s^{t-1}\}$ . Formons maintenant un tableau de  $s$  lignes et  $s^t$  colonnes (nous numérotions les lignes de 0 à  $s-1$  et les colonnes de 0 à  $s^{t-1}$ ) de la façon suivante : dans la  $i$ ème ligne et la  $j$ ème colonne nous mettons le nombre  $u$  tel que  $y_j(e_i) = e_u$ . Le tableau ainsi formé est un tableau orthogonal d'indice unité. En effet, si nous pouvions trouver  $t$  lignes telles que  $2^t$ -uples soient identiques (par exemple dans les colonnes  $j$  et  $j'$  et pour les lignes correspondant à  $e_{i_1}, e_{i_2}, \dots, e_{i_t}$  respectivement) nous aurions :

$$y_j(e_{i_k}) = y_{j'}(e_{i_k}) \quad \forall e_{i_k} \in \{e_{i_1}, e_{i_2}, \dots, e_{i_t}\}$$

ce qui nous donnerait des équations de la forme :

$$\sum_{l=0}^{t-1} A_l e_{i_k}^l = 0$$

Soient  $t$  équations linéaires et homogènes en  $A_{t-1}, A_{t-2}, \dots, A_1, A_0$ .

Or tous les  $A_l$  ne sont pas nuls puisque les polynômes  $y_j(x)$  et  $y_{j'}(x)$  sont distincts. Donc si le système a une solution, le déterminant de la matrice  $V$  définie ci-dessous doit être nul :



$V = (e_{i_k}^1)$ ,  $e_{i_k}^1$  étant l'élément qui se trouve à la kème ligne et à la lème colonne (la matrice  $V$  est donc une matrice de  $t$  lignes ( $k = 0, 1, 2, \dots, t-1$ ) et de  $t$  colonnes ( $l = 0, 1, 2, \dots, t-1$ )).

Or, on voit que  $\det(V) = \prod_{u < v} (e_{i_u} - e_{i_v})$  (déterminant de Vandermonde) et donc  $\det(V)$  ne saurait être nul. De plus, nous pouvons ajouter une ligne au tableau ainsi construit. En effet, nous mettons dans cette ligne le nombre  $u$  dans les colonnes correspondant aux polynômes dont les coefficients de  $x^{t-1}$  sont  $e_u$ . Vérifions alors que, prenant  $t$  lignes parmi lesquelles se trouve celle que nous venons de construire, il n'y a pas dans les colonnes du sous-tableau considéré 2  $t$ -uples identiques. Ces 2  $t$ -uples ne pourraient provenir que de colonnes dans lesquelles on a le même nombre  $u$  dans la dernière ligne. Alors, en reprenant les notations précédentes, on aurait  $A_{t-1} = 0$  et nous aurions un système de  $t-1$  équations à  $t-1$  inconnues. Le système étant un système d'équations homogènes, il faudrait, pour qu'il existe une solution, que le déterminant de ce système soit nul. Or le déterminant obtenu est aussi un déterminant de Vandermonde qui ne saurait être nul. Nous avons donc bien obtenu un tableau orthogonal  $(1, s+1, s, t)$ .

Remarque II.5.1 : Dans le cas où  $t = 3$ , on peut ajouter une ligne si  $s = 2^n$ .

En effet, construisons la ligne où l'on met dans les colonnes correspondant aux polynômes dont le coefficient de  $x$  est  $e_u$ , le nombre  $u$ . Alors si on prend 2 triplets de la sous-matrice constituée par les 2 dernières lignes et une autre ligne prise parmi les  $s$  premières, ces 2 triplets ne pourront être identiques que si les éléments correspondant aux 2 dernières lignes sont identiques, et, toujours avec les mêmes notations que celles que nous venons d'employer,  $A_2 = A_1 = 0$  et on obtient une équation à une inconnue :  $A_0 = 0$  ce qui est exclu.

Si on prend 2 triplets de la matrice constituée par la ligne que nous venons de construire et 2 lignes prises parmi les  $s$  premières,



celles qui correspondent à  $e_{i_m}$  et  $e_{i_k}$  par exemple, on obtient un système de 2 équations à 2 inconnues (équations homogènes) dont le déterminant est :

$$\begin{vmatrix} e_{i_m}^2 & 1 \\ e_{i_k}^2 & 1 \end{vmatrix} = (e_{i_m} - e_{i_k})(e_{i_m} + e_{i_k})$$

Or dans  $GF(2^n)$  on ne peut avoir  $e_{i_k} + e_{i_m} = 0$  puisque cela entraînerait  $e_{i_k} = e_{i_m}$ .

II.5.2 : Construction de tableaux orthogonaux ( $\lambda = s^m, r, s=p^n, t$ )  
(p étant un nombre entier, m et n 2 entiers  
quelconques [III])

Théorème II.5.2 : S'il existe une matrice  $C = (c_{ij})$  de r lignes et de (m+t) colonnes ( $i = 1, 2, \dots, r$  ;  $j = 1, 2, \dots, m+t$ ) dont les éléments appartiennent au corps de Galois  $GF(p^n)$ , et telle que toute sous-matrice obtenue en prenant t lignes est de rang t, alors on peut construire un tableau orthogonal ( $\lambda = s^m, r, s=p^n, t$ ). (p = nombre premier).

Démonstration : Considérons les  $s^{m+t}$  vecteur-colonnes d'ordre (m+t) qu'il est possible de construire à l'aide des éléments de  $GF(p^n)$ . Soit  $\xi_k$  ( $k = 1, 2, \dots, s^{m+t}$ ) un de ces vecteurs et soit A le tableau constitué par la juxtaposition des  $s^{m+t}$  vecteur-colonnes  $C \cdot \xi_k$ . Nous allons montrer que A est le tableau orthogonal cherché. En effet, soit A' une sous-matrice de A formée de t lignes de A et soit C' la sous-matrice de C (t lignes, m+t colonnes) correspondant à A'.

Les colonnes  $\alpha_k$  de A' sont telles que  $\alpha_k = C' \cdot \xi_k$  et comme C' est de rang t, chaque  $\alpha_k$  est obtenu à partir de  $s^m$  différents vecteurs  $\xi$ . Donc dans A', chaque vecteur colonne intervient avec la fréquence  $\lambda = s^m$ , ce qui montre que A est un tableau orthogonal ( $s^m, r, s, t$ ).



### III - CONSTRUCTION DE TABLEAUX ORTHOGONAUX

#### A PARTIR D'AUTRES TABLEAUX ORTHOGONAUX

#### III.1 : Construction de tableaux orthogonaux par "produit direct"

Théorème III.1. : S'il existe un tableau orthogonal  $(\lambda_1, r, S_1, t)$  et un tableau orthogonal  $(\lambda_2, r, S_2, t)$ , alors on peut construire un tableau orthogonal  $(\lambda_1 \lambda_2, r, S_1 S_2, t)$ .

Démonstration : En effet, soit  $a_{ij}$  l'élément de la  $i$ ème ligne et de la  $j$ ème colonne du 1er tableau A ;  $a_{ij} \in E$  ;  $\text{card } E = S_1$ . Soit  $b_{ik}$  l'élément de la  $i$ ème ligne et de la  $k$ ème colonne du 2ème tableau B ;  $b_{ik} \in F$  ;  $\text{card } F = S_2$ . Nous construisons un 3ème tableau C dont l'élément  $c_{i,jk}$  de la  $i$ ème ligne et de la  $(jk)$ ème colonne est  $c_{i,jk} = (a_{ij}, b_{ik}) \in E \times F$ .

Nous allons montrer que le tableau de  $r$  lignes et  $\lambda_1 \lambda_2 (S_1 S_2)^t$  colonnes ainsi construit sur  $E \times F$  est bien un tableau orthogonal de force  $t$ , de  $r$  lignes et d'indice  $\lambda_1 \lambda_2$ .

Considérons  $t$  lignes d'indices  $i_1, i_2, \dots, i_t$ . le  $t$ -uple :

$(a_{i_1 j}, a_{i_2 j}, \dots, a_{i_t j})$  décrit  $\lambda_1$  fois  $E^t$  lorsque  $j$  prend les

$\lambda_1 S_1^t$  valeurs possibles puisque A est un tableau orthogonal.

Le  $t$ -uple  $(b_{i_1 k}, b_{i_2 k}, \dots, b_{i_t k})$  décrit  $\lambda_2$  fois  $F^t$  lorsque  $k$  prend les  $\lambda_2 S_2^t$  valeurs possibles puisque B est un tableau orthogonal. Il en résulte que le  $t$ -uple :

$[(a_{i_1 j}, b_{i_1 k}), (a_{i_2 j}, b_{i_2 k}), \dots, (a_{i_t j}, b_{i_t k})]$

décrit  $\lambda_1 \lambda_2$  fois  $(E \times F)^t$  lorsque  $(j, k)$  prend les  $\lambda_1 S_1^t \lambda_2 S_2^t$

valeurs possibles. Le tableau ainsi construit sur  $E \times F$  est donc bien un tableau orthogonal de force  $t$ , de  $r$  lignes et d'indice  $\lambda_1 \lambda_2$ .



Corollaire III.1.1 - Le nombre maximum de contraintes d'un tableau orthogonal de type  $(1, r, S, t)$ , où  $S = S_1 S_2$ , est toujours supérieur ou égal au minimum des 2 nombres  $r_1 \text{ max.}$  et  $r_2 \text{ max.}$ , où  $r_1 \text{ max.}$  désigne le nombre maximum de contraintes d'un tableau orthogonal de type  $(1, r_1, S_1, t)$  et  $r_2 \text{ max.}$  désigne le nombre maximum de contraintes d'un tableau orthogonal de type  $(1, r_2, S_2, t)$ .

III.2.: Construction de tableaux orthogonaux par la méthode de Yamamoto modifiée et étendue aux tableaux orthogonaux de force quelconque : [XIV] et [XXII]

Théorème III.2.1 : Etant donnés un tableau orthogonal  $(1, 2t+1, s_1, t)$  et un tableau orthogonal  $(1, t+2, s_2, t)$ , si  $s_1 > 2 s_2$ , il est possible de construire un tableau orthogonal  $(2^{t-1}(t-1)!, t+2, s_1 + s_2, t)$  qui admet le tableau  $(1, t+2, s_2, t)$  comme sous-tableau orthogonal.

Démonstration : Soit  $E = \{x_i ; i = 1, 2, \dots, s_1\}$  et soit  $F = \{y_i ; i = 1, 2, \dots, s_2\}$ . Puisque  $s_1 > 2 s_2$ , il existe deux sous-ensembles  $\Gamma \subset E$  et  $\Theta \subset E$  tels que :

$$\Gamma = \{\gamma_i ; i = 1, 2, \dots, s_2\}$$

$$\Theta = \{\theta_i ; i = 1, 2, \dots, s_2\} \quad \text{et} \quad \Gamma \cap \Theta = \emptyset$$

Reprenons les notations de I.5 et soit  $T_E$  le tableau orthogonal  $(1, 2t+1, S_1, t)$  construit sur  $E$  et dont la suite des colonnes est :  $(X, S_1(X), S_2(X), \dots, S_{t-1}(X), \Phi(X), \Phi'(X))$  où  $X$  décrit  $E^t$ .

De la même façon, soit  $T_F$  le tableau orthogonal  $(1, t+2, s_2, t)$  construit sur  $F$  et dont la suite des colonnes est :



$(Y, \psi(Y), \psi'(Y))$  où  $Y$  décrit  $F^t$

Nous nous proposons de construire à partir de  $T_E$  et  $T_F$  un tableau orthogonal  $T_{EUF}$  sur l'ensemble  $E \cup F$ .

Le tableau  $T_{EUF}$  que nous construisons est constitué par :

1°) chacune des colonnes de  $T_F$  comptée  $2^{t-1}(t-1)!$  fois, ce qui nous donne en tout

$$2^{t-1}(t-1)! s_2^t \text{ colonnes.}$$

2°) si le  $t$ -uplet  $Z$  constitué par la suite des éléments des  $t$  premières lignes appartient à  $F^{t-1}E$ , par exemple :

$Z = (y_{i_1}, y_{i_2}, \dots, y_{i_{t-1}}, x_{i_t})$ , nous mettrons alors dans le tableau la colonne suivante :

$$(Z, \Phi(x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, x_{i_t}), \Phi'(x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, x_{i_t}))$$

dans laquelle les  $x_{j_f}$  ( $f = 1, 2, \dots, t-1$ ) sont déterminés par le système  $S \pi(i_m) (x_{j_1}, x_{j_2}, \dots, x_{j_{t-1}}, x_{i_t}) = \lambda_{i_m}$  ( $m = 1, 2, \dots, t-1$ )

où  $\lambda_{i_m} = \gamma_{i_m}$  ou  $\theta_{i_m}$  et où  $\pi$  est une application injective de l'ensemble  $\{i_m ; m = 1, 2, \dots, t-1\}$  dans l'ensemble  $\{1, 2, \dots, t-1\}$ .

(On sait que  $T_E$  étant un tableau orthogonal de force 1, les  $x_{j_f}$  sont ainsi déterminés de façon unique).

Le choix " $\gamma_{i_m}$  ou  $\theta_{i_m}$ " donne  $2^{t-1}$  possibilités et il existe  $(t-1)!$  applications  $\pi$ , ce qui nous donne en épuisant toutes les possibilités  $2^{t-1}(t-1)!$  colonnes à  $Z$  donné.

Lorsque varient les composantes de  $Z$  on obtient  $2^{t-1}(t-1)! s_2^{t-1} s_1$  colonnes, et comme il existe  $C_t^{t-1}$   $t$ -uplets analogues à  $Z$ , ne différant de ce dernier que par la place de  $x$  parmi les  $t$  premières lignes, nous obtenons en tout  $C_t^{t-1} 2^{t-1}(t-1)! s_2^{t-1} s_1$  colonnes



$$(C_p^q = p!/q! (p-q)! \quad \text{pour } p \geq q).$$

3°) si le  $t$ -uplet  $Z$  constitué par la suite des éléments des  $t$  premières lignes appartient à  $F^{t-n} E^n$  ( $1 < n \leq t$ ), soit par exemple :

$$Z = (y_{i_1}, y_{i_2}, \dots, y_{i_{t-n}}, x_{i_{t-n+1}}, x_{i_{t-n+2}}, \dots, x_{i_t})$$

on choisira  $\lambda_{i_m} = \gamma_{i_m}$  ou  $\theta_{i_m}$  ( $m = 1, 2, \dots, t-n$ )

et une application injective  $\pi$  de l'ensemble  $\{i_m ; m = 1, 2, \dots, t-n\}$  dans l'ensemble  $\{1, 2, \dots, t-1\}$ . Une fois ces deux choix faits, on déterminera  $X = (x_{j_1}, x_{j_2}, \dots, x_{j_{t-n}})$  solution unique du

système  $S_{\pi(i_m)} (X, x_{i_{t-n+1}}, x_{i_{t-n+2}}, \dots, x_{i_t}) = \lambda_{i_m} \quad (m=1, \dots, t-n)$

soit alors  $\{T_1, T_2, \dots, T_{n-1}\}$  le complément de l'ensemble

$\{S_{\pi(i_m)} ; m = 1, 2, \dots, t-n\}$  dans l'ensemble  $\{S_1, S_2, \dots, S_{t-1}\}$

On a alors :

$$T_1(X, x_{i_{t-n+1}}, x_{i_{t-n+2}}, \dots, x_{i_t}) = \mu_{i_1} \quad (1 = 1, 2, \dots, n-1)$$

et plusieurs cas peuvent se produire :

ou bien  $\mu_{i_1} \in \Gamma$ , ou bien  $\mu_{i_1} \in \ominus$ , ou bien  $\mu_{i_1} \in \Gamma \cap \ominus$

Supposons que parmi les  $(n-1)$   $\mu_{i_1}$  il y en ait  $k$  qui appartiennent à  $\Gamma \cap \ominus$  et donc  $n - k - 1$  qui sont soit des  $\gamma$ , soit des  $\theta$ .

Par exemple, supposons que :

$$\mu_{i_1} = \gamma_{r_1}, \dots, \mu_{i_v} = \gamma_{r_v}, \mu_{i_{v+1}} = \theta_{r_{v+1}}, \dots, \mu_{i_{n-k-1}} = \theta_{r_{n-k-1}}$$

Dans ce cas, nous mettrons dans  $T_{EUF}$  les colonnes suivantes ;



- (I)  $\left( Z, \Phi(X, x_{i_{t-n+1}}, x_{i_{t-n+2}}, \dots, x_{i_t}), \Phi'(X, x_{i_{t-n+1}}, x_{i_{t-n+2}}, \dots, x_{i_t}) \right)$
- (II)  $\left( Z, y_{r_\sigma}, y_{r_\tau} \right) \quad (\sigma = 1, 2, \dots, n-k-1; \tau = 1, 2, \dots, n-k-1) \quad \sigma \neq \tau$
- (III)  $\left( Z, \Phi(X, x_{i_{t-n+1}}, x_{i_{t-n+2}}, \dots, x_{i_t}), y_{r_\sigma} \right) \quad (\sigma = 1, 2, \dots, n-k-1)$
- (IV)  $\left( Z, y_{r_\sigma}, \Phi'(X, x_{i_{t-n+1}}, x_{i_{t-n+2}}, \dots, x_{i_t}) \right) \quad (\sigma = 1, 2, \dots, n-k-1)$

La colonne (I) sera comptée :

$$2^{n-1}(n-1)! - 2(n-1-k) A(n,k) + (n-1-k)(n-2-k) B(n,k) \text{ fois.}$$

Chacune des  $(n-1-k)(n-2-k)$  colonnes (II) sera comptée  $B(n,k)$  fois.

Chacune des  $(n-1-k)$  colonnes (III) sera comptée :

$$A(n,k) - (n-2-k) B(n,k) \text{ fois;}$$

Chacune des  $(n-1-k)$  colonnes (IV) sera comptée :

$$A(n,k) - (n-2-k) B(n,k) \text{ fois.}$$

Avec :

$$A(n,k) = \sum_{u=0}^{n-1} \sum_{i=0}^u \sum_{j=1}^{n-k-i-1} (-1)^{j+1} C_k^{u-i} \frac{(n-j-1)!(n-k-i-2)!}{(n-j-k-i-1)!} C_{n-k-2}^i$$

$$\text{où } k \leq n-2, \quad C_p^q = \frac{p!}{q!(p-q)!} \text{ si } p \geq q, \quad C_p^q = 0 \text{ si } p < q, \quad C_0^0 = 1, \quad 0! = 1$$

$$B(n,k) = (n-k-3)! \sum_{u=2}^{n-k-1} (-1)^u 2^{n-u-1} \frac{(n-u-1)!}{(n-k-u-1)!} (u-1)$$

$$\text{où } k \leq n-3 \quad B(n,n-2) = B(n,n-1) = 0 = A(n,n-1)$$

A Z donné on fait ainsi correspondre (le choix de  $\pi$  et le choix " $\chi$  ou  $\theta$ " étant fait) :

$$2^{n-1}(n-1)! - 2(n-1-k) A(n,k) + (n-1-k)(n-2-k) B(n,k)$$

$$+ (n-1-k)(n-2-k) B(n,k)$$

$$+ 2(n-1-k) [A(n,k) - (n-2-k) B(n,k)] \text{ colonnes}$$



Soit en tout  $2^{n-1}(n-1)!$  colonnes.

Le choix " $\gamma_{i_m}$  ou  $\theta_{i_m}$ " donne  $2^{t-n}$  possibilités et il existe

$\frac{(t-1)!}{(n-1)!}$  applications  $\pi$ , ce qui nous donne en épuisant toutes les possibilités  $2^{t-1}(t-1)!$  colonnes, à  $Z$  donné.

Lorsque varient les composantes de  $Z$ , on obtient  $2^{t-1} s_2^{t-n} s_1^n (t-1)!$  colonnes et comme il existe  $C_t^{t-n}$   $t$ -uples analogues à  $Z$ , ne différant de ce dernier que par la place des  $x$  dans les  $t$  premières lignes, nous obtenons en tout  $C_t^{t-n} 2^{t-1}(t-1)! s_2^{t-n} s_1^n$  colonnes.

Nous venons de construire un tableau  $T_{EUF}$  qui possède

$$\sum_{n=0}^{n=t} C_t^{t-n} 2^{t-1}(t-1)! s_2^{t-n} s_1^n = 2^{t-1}(t-1)! (s_1 + s_2)^n \text{ colonnes.}$$

Il reste à prouver que  $T_{EUF}$  est un tableau orthogonal

$$(2^{t-1}(t-1)!, t+2, s_1 + s_2, t).$$

. Si nous considérons les  $t$ -uples constitués par les éléments des  $t$  premières lignes du tableau, la méthode de construction même nous montre que chacun de ces  $t$ -uples figure dans le tableau et est répété  $2^{t-1}(t-1)!$  fois.

. Calculons le nombre de répétitions d'un  $t$ -uple constitué par les éléments des lignes d'ordre 1, 2, ...,  $t-2$ ,  $t+1$ , et  $t+2$ , éléments qui sont respectivement  $y_{i_1}, y_{i_2}, \dots, y_{i_{t-n}}, x_{i_{t-n+1}}, \dots,$

$$x_{i_{t-2}}, y_i \text{ et } y_j.$$

La méthode de construction décrite ci-dessus nous montre qu'un tel  $t$ -uple,  $\pi$  étant choisi, le choix  $\lambda_{i_m} = (\theta_{i_m} \text{ ou } \gamma_{i_m})$  étant fait, ne peut provenir que des  $2^2 \frac{(n-1)!}{(n-3)!}$   $t$ -uples de  $T_E$  dont les éléments  $\lambda_{i_1}, \lambda_{i_2}, \dots, \lambda_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-2}}, \lambda_i$  et  $\lambda_j$

se trouvent respectivement dans les lignes  $S_{\pi(1)}, S_{\pi(2)}, \dots, S_{\pi(t-n)}$   $t-n+1, \dots, t-2, T_u$  et  $T_v$  où  $\lambda_i = \gamma_i$  ou  $\theta_i$ ,  $\lambda_j = \gamma_j$  ou  $\theta_j$



et où  $T_u$  et  $T_v$  sont 2 éléments de l'ensemble  $\{T_1, T_2, \dots, T_{n-1}\}$ .

Or  $n$  étant fixé et le choix  $\lambda_{i_m} = (\gamma_{i_m} \text{ ou } \theta_{i_m})$  étant fait,

un tel  $t$ -uplet peut être tel que  $Z \in F^{t-n} E^n$  et le nombre de répétitions est alors  $2^2 \frac{(n-1)!}{(n-3)!} B(n, k)$ , ou tel que

$Z \in F^{t-n} E^{n-2} E F$  ou  $F^{t-n} E^{n-2} F E$ , le nombre de répétitions étant

alors  $2^2 \frac{(n-1)!}{(n-3)!} 2(n-3-k) B(n-1, k)$  ou enfin tel que

$Z \in F^{t-n} E^{n-2} F^2$  et le nombre de répétitions est alors

$2^2 \frac{(n-1)!}{(n-3)!} (n-k-3)(n-4-k) B(n-2, k)$  soit en tout :

$2^2 \frac{(n-1)!}{(n-3)!} B(n, k) + 2(n-k-3) B(n-1, k) + (n-k-3)(n-k-4) B(n-2, k)$

$= 2^2 \frac{(n-1)!}{(n-3)!} \cdot B$

Or  $B = (n-k-3)! \sum_{u=2}^{n-k-1} (-1)^u 2^{n-u-1} \frac{(n-u-1)!}{(n-u-k-1)!} (u-1)$

$+ 2(n-k-3)! \sum_{u=2}^{n-k-2} (-1)^u 2^{n-u-2} \frac{(n-u-2)!}{(n-k-u-2)!} (u-1)$

$+ (n-k-3)! \sum_{u=2}^{n-k-3} (-1)^u 2^{n-u-3} \frac{(n-u-3)!}{(n-k-u-3)!} (u-1)$

Soit encore :

$B = (n-k-3)! \sum_{u=2}^{n-k-1} (-1)^u 2^{n-u-1} \frac{(n-u-1)!}{(n-k-u-1)!} (u-1)$

$+ (n-k-3)! \sum_{u=3}^{n-k-1} (-1)^{u-1} 2^{n-u-1} \frac{(n-u-1)!}{(n-k-u-1)!} (u-2)$

$+ (n-k-3)! \sum_{u=4}^{n-k-1} (-1)^{u-2} 2^{n-u-1} \frac{(n-u-1)!}{(n-k-u-1)!} (u-3)$



$$\begin{aligned}
\text{d'où } B &= 2^{n-3} \frac{(n-3)!}{(n-k-3)!} (n-k-3)! \\
&- 2 \cdot 2^{n-4} \frac{(n-4)!}{(n-k-4)!} (n-k-3)! \\
&+ 2 \cdot 2^{n-4} \frac{(n-4)!}{(n-k-4)!} (n-k-3)! \\
&+ (n-k-3)! \sum_{u=4}^{n-k-1} (-1)^{u-2} 2^{n-u-1} \frac{(n-u-1)!}{(n-k-u-1)!} \left[ (u-1) - 2(u-2) + (u-3) \right]
\end{aligned}$$

$$\text{Soit } B = 2^{n-3} (n-3)!$$

et donc  $\lambda$  étant fixé et le choix  $\lambda_{i_m} = (\gamma_{i_m} \text{ ou } \theta_{i_m})$  étant fait, on obtient  $2^2 \frac{(n-1)!}{(n-3)!} 2^{n-3} (n-3)! = 2^{n-1} (n-1)!$  répétitions du  $t$ -uplet considéré. Ce nombre ne dépendant pas de  $k$ , il en résulte que lorsque l'on prend toutes les possibilités pour  $\lambda$  et pour  $\lambda_{i_m}$ , on obtient en tout  $2^{t-1} (t-1)!$  répétitions du  $t$ -uplet considéré. De plus,  $T_E$  étant un tableau orthogonal de force  $t$  et d'indice 1, la méthode appliquée montre que tous les  $t$ -uplets tels que celui que nous venons de considérer figurent dans  $T_{EUF}$ .

Il est enfin évident que le raisonnement fait s'applique quelle que soit la place occupée par les  $(t-n)$   $y$  dans les  $t$  premières lignes.

. Calculons maintenant le nombre de répétitions d'un  $t$ -uplet constitué par les éléments des lignes d'ordre 1, 2, ...,  $t-2$ ,  $t+1$  et  $t+2$ , éléments qui sont respectivement  $y_{i_1}, y_{i_2}, \dots, y_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-2}}, y_i$  et  $x_j$ . La méthode de construction montre qu'un  $t$ -uplet ne peut provenir que des  $2 \cdot \frac{(n-1)!}{(n-2)!}$   $t$ -uplets de  $T_E$  dont les éléments,  $\lambda$  étant fixé et le choix  $\lambda_{i_m} = (\gamma_{i_m} \text{ ou } \theta_{i_m})$  étant fait,  $\lambda_{i_1}, \lambda_{i_2}, \dots, \lambda_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-2}}, \lambda_i$  et  $x_j$  se trouvent respectivement dans les lignes.



$S \pi(1), S \pi(2), \dots, S \pi(t-n), t-n+1, \dots, t-2, T_u$  et  $\Phi'$   
 où  $\lambda_i = \gamma_i$  ou  $\theta_i$  et où  $T_u$  est un élément de  $\{T_1, T_2, \dots, T_{n-1}\}$ .

Or un tel  $t$ -uple peut être tel que  $Z \in F^{t-n} E^n$  et le nombre de répétitions est alors  $2 \frac{(n-1)!}{(n-2)!} (A_{(n,k)} - (n-2-k) B_{(n,k)})$ , ou bien tel que  $Z \in F^{t-n} E^{n-2} EF$  ou  $F^{t-n} E^{n-2} FE$ , le nombre de répétitions étant alors :

$$2 \frac{(n-1)!}{(n-2)!} - 2(n-2-k) (A_{(n-1,k)} - (n-k-3) B_{(n-1,k)})$$

ou bien tel que  $Z \in F^{t-n} E^{n-2} F^2$  et le nombre de répétitions est alors :

$$\begin{aligned} & (n-2-k)(n-3-k) (A_{(n-2,k)} - (n-k-4) B_{(n-2,k)}), \text{ soit en tout :} \\ & 2 \frac{(n-1)!}{(n-2)!} [A_{(n,k)} + 2(n-2-k) A_{(n-1,k)} + (n-2-k)(n-3-k) A_{(n-2,k)}] \\ & - 2 \frac{(n-1)!}{(n-2)!} [(n-2-k) B_{(n,k)} + 2(n-3-k) B_{(n-1,k)} + (n-3-k)(n-4-k) B_{(n-2,k)}] \\ & = 2 \frac{(n-1)!}{(n-2)!} [A_{(n,k)} + 2(n-2-k) A_{(n-1,k)} + (n-2-k)(n-3-k) A_{(n-2,k)}] \\ & - 2^{n-2} \frac{(n-1)!}{(n-2)!} (n-2-k)(n-3)! \text{ d'après des calculs précédents} \end{aligned}$$

Posons  $A = A_{(n,k)} + 2(n-2-k) A_{(n-1,k)} + (n-2-k)(n-3-k) A_{(n-2,k)}$

$$\begin{aligned} A &= \sum_{u=0}^{n-1} \sum_{i=0}^u \sum_{j=1}^{n-k-i-1} (-1)^{j+1} C_k^{u-i} C_{n-k-2}^i \frac{(n-j-1)!(n-k-i-2)!}{(n-j-k-i-1)!} \\ &+ 2(n-2-k) \sum_{u=0}^{n-2} \sum_{i=0}^u \sum_{j=1}^{n-k-i-2} (-1)^{j+1} C_k^{u-i} C_{n-k-3}^i \frac{(n-j-2)!(n-k-i-3)!}{(n-j-k-i-2)!} \\ &+ (n-2-k)(n-3-k) \sum_{u=0}^{n-3} \sum_{i=0}^u \sum_{j=1}^{n-k-i-3} (-1)^{j+1} C_k^{u-i} C_{n-k-4}^i \frac{(n-j-3)!(n-k-i-4)!}{(n-j-k-i-3)!} \\ &= \sum_{u=0}^{n-1} \sum_{i=0}^u \sum_{j=1}^{n-k-i-1} (-1)^{j+1} C_k^{u-i} \frac{(n-j-1)!}{i!(n-j-k-i-1)!} \end{aligned}$$



$$\begin{aligned}
& + 2 \sum_{u=0}^{n-2} \sum_{i=0}^u \sum_{j=1}^{n-k-i-2} (-1)^{j+1} C_k^{u-i} \frac{(n-j-2)!}{i!(n-j-k-i-2)!} \\
& + \sum_{u=0}^{n-3} \sum_{i=0}^u \sum_{j=1}^{n-k-i-3} (-1)^{j+1} C_k^{u-i} \frac{(n-j-3)!}{i!(n-j-k-i-3)!} \\
& = \sum_{u=0}^{n-1} \sum_{i=0}^u \sum_{j=1}^{n-k-i-1} (-1)^{j+1} C_k^{u-i} \frac{(n-j-1)!}{i!(n-j-k-i-1)!} \\
& + 2 \sum_{u=0}^{n-2} \sum_{i=0}^u \sum_{j=2}^{n-k-i-1} (-1)^j C_k^{u-i} \frac{(n-j-1)!}{i!(n-j-k-i-1)!} \\
& + \sum_{u=0}^{n-3} \sum_{i=0}^u \sum_{j=3}^{n-k-i-1} (-1)^{j-1} C_k^{u-i} \frac{(n-j-1)!}{i!(n-j-k-i-1)!}
\end{aligned}$$

et après réduction des termes semblables, on a :

$$\begin{aligned}
A &= \sum_{u=n-2}^{n-1} \sum_{i=0}^u \sum_{j=1}^2 (-1)^{j+1} C_k^{u-i} C_{n-k-2}^i \frac{(n-j-1)!(n-k-i-2)!}{(n-j-k-i-1)!} \\
& + 2 \sum_{u=n-2}^{n-2} \sum_{i=0}^u \sum_{j=2}^2 (-1)^j C_k^{u-i} C_{n-k-2}^i \frac{(n-j-1)!(n-k-i-2)!}{(n-j-k-i-1)!} \\
& + \sum_{u=0}^{n-3} \sum_{i=0}^u \sum_{j=1}^2 (-1)^{j+1} C_k^{u-i} C_{n-k-2}^i \frac{(n-j-1)!(n-k-i-2)!}{(n-k-i-j-1)!} \\
& + 2 \sum_{u=0}^{n-3} \sum_{i=0}^u \sum_{j=2}^2 (-1)^j C_k^{u-i} C_{n-k-2}^i \frac{(n-j-1)!(n-k-i-2)!}{(n-k-i-j-1)!} \\
& = (n-2)! + 0 + (n-2)! (2^{n-2} - 1) \\
& - \sum_{u=0}^{n-3} \sum_{i=0}^u C_k^{u-i} C_{n-k-2}^i (n-3)! (n-k-i-2) \\
& + 2 \sum_{u=0}^{n-3} \sum_{i=0}^u C_k^{u-i} C_{n-k-2}^i (n-3)! (n-k-i-2)
\end{aligned}$$



$$\begin{aligned}
&= 2^{n-2} (n-2)! + (n-3)! \sum_{u=0}^{n-3} \sum_{i=0}^u C_k^{u-i} C_{n-k-2}^i (n-k-i-2) \\
&= 2^{n-2} (n-2)! + (n-3)! (n-k-2) \sum_{u=0}^{n-3} \sum_{i=0}^u C_k^{u-i} C_{n-k-2-(n-3)}^i \sum_{u=0}^{n-3} \sum_{i=0}^u C_k^{u-i} C_{n-k-2}^i \\
&= 2^{n-2} (n-2)! + \sum_{u=0}^{n-3} C_{n-2}^u (n-3)! (n-k-2) - (n-3)! \sum_{u=0}^{n-3} C_{n-3}^{u-1} (n-k-2)
\end{aligned}$$

$$A = 2^{n-2} (n-2)! + (n-3)! (n-k-2) (2^{n-2} - 1) - (n-3)! (n-k-2) (2^{n-3} - 1)$$

$$A = 2^{n-2} (n-2)! + (n-3)! (n-k-2) 2^{n-3}$$

et donc  $\lambda$  étant fixé et le choix  $\lambda_{i_m} = (\gamma_{i_m} \text{ ou } \theta_{i_m})$  étant fait,

$$\text{on obtient } 2 \frac{(n-1)!}{(n-2)!} \left[ 2^{n-2} (n-2)! + (n-3)! (n-k-2) 2^{n-3} \right]$$

$$- 2^{n-2} \frac{(n-1)!}{(n-2)!} (n-2-k)(n-3)! = 2^{n-1} (n-1)! \text{ répétitions du}$$

t-uple considéré. Ce nombre ne dépendant pas de  $k$ , il en résulte que, lorsque l'on prend toutes les possibilités pour  $\lambda$  et pour  $\lambda_{i_m}$ , on obtient en tout  $2^{t-1} (t-1)!$  répétitions du t-uple considéré. De plus  $T_E$  étant un tableau orthogonal de force  $t$  et d'indice 1, la méthode montre que tous les t-uples tels que celui que nous venons de considérer figurent dans  $T_{EUF}$ . Il est enfin évident que le raisonnement fait s'applique quelle que soit la place occupée par les  $(t-n)$   $y$  dans les  $t$  premières lignes.

. Le même raisonnement que celui que nous venons de faire montre que le nombre de répétitions d'un t-uple constitué par les éléments des lignes d'ordre 1, 2, ...,  $t-2$ ,  $t+1$  et  $t+2$ , éléments qui sont respectivement  $y_{i_1}, y_{i_2}, \dots, u_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-2}}, x_i$  et  $y_j$  est  $2^{t-1} (t-1)!$ .



. Calculons le nombre de répétitions d'un  $t$ -uplet constitué par les éléments des lignes d'ordre  $1, 2, \dots, t-2, t+1$  et  $t+2$ , éléments qui sont respectivement  $y_{i_1}, y_{i_2}, \dots, y_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-2}}, x_i$  et  $x_j$ . La méthode de construction montre qu'un tel  $t$ -uplet ne peut provenir que du  $t$ -uplet de  $T_E$  dont les éléments,  $\pi$  étant fixé et le choix  $\lambda_{i_m} = (\gamma_{i_m} \text{ ou } \theta_{i_m})$  étant fait,  $\lambda_{i_1}, \lambda_{i_2}, \dots, \lambda_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-2}}, x_i$  et  $x_j$  se trouvent respectivement dans les lignes  $S_{\pi(1)}, S_{\pi(2)}, \dots, S_{\pi(t-n)}, t-n+1, \dots, t-2, \Phi$  et  $\Phi'$ . Or un tel  $t$ -uplet peut être tel que  $Z \in F^{t-n} E^n$  et dans ce cas le nombre de répétitions sera :

$$2^{n-1}(n-1)! - 2(n-1-k) A_{(n,k)} + (n-1-k)(n-2-k) B_{(n,k)}$$

ou bien tel que  $Z \in F^{t-n} E^{n-2} E F$  ou  $F^{t-n} E^{n-2} F E$  et le nombre de répétitions sera alors :

$$2(n-1-k) \left[ 2^{n-2}(n-2)! - 2(n-2-k) A_{(n-1,k)} + (n-2-k)(n-3-k) B_{(n-1,k)} \right]$$

ou bien tel que  $Z \in F^{t-n} E^{n-2} F^2$  et ce nombre de répétitions sera alors :

$$(n-1-k)(n-2-k) \left[ 2^{n-3}(n-3)! - 2(n-3-k) A_{(n-2,k)} + (n-3-k)(n-4-k) B_{(n-2,k)} \right]$$

soit en tout :

$$2^{n-1}(n-1)! + (n-1-k) 2^{n-1}(n-2)! + (n-1-k)(n-2-k) 2^{n-3}(n-3)!$$

$$- 2(n-1-k) A + (n-1-k)(n-2-k) B$$

$= 2^{n-1}(n-1)!$  ce qui en utilisant toutes les possibilités pour  $\pi$  et pour  $\lambda_{i_m}$  nous donne  $2^{t-1}(t-1)!$  répétitions. On constate

de plus que tous les  $t$ -uplets tels que celui considéré figurent dans



$T_{EUF}$  et que le raisonnement est indépendant de la place occupée par les  $(t-n)$  y dans les  $t$  premières lignes.

. Calculons le nombre de répétitions d'un  $t$ -uplet constitué par les éléments des lignes d'ordre 1, 2, ...,  $t-1$  et  $t+1$ , éléments qui sont respectivement  $y_{i_1}, y_{i_2}, \dots, y_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-1}}$  et  $x_{i_t}$ . D'une manière analogue à celle que nous venons d'appliquer plusieurs fois et en utilisant les mêmes notations, on montre que, à  $n$  fixé et le choix  $\lambda_{i_m} = \gamma_{i_m}$  ou  $\theta_{i_m}$  étant fait pour les  $t-n$  composantes  $\in F$ , le nombre de répétitions est

$$\begin{aligned}
 & 2^{n-1}(n-1)! - 2(n-1-k) A_{(n,k)} + (n-1-k)(n-2-k) B_{(n,k)} \\
 & + \left[ 2^{n-2}(n-2)! - 2(n-2-k) A_{(n-1,k)} + (n-2-k)(n-3-k) B_{(n-1,k)} \right] (n-k-1) \\
 & + \left[ A_{(n,k)} - (n-2-k) B_{(n,k)} \right] (n-1-k) \\
 & + \left[ A_{(n-1,k)} - (n-3-k) B_{(n-1,k)} \right] (n-1-k)(n-2-k) \\
 & = 2^{n-1}(n-1)! + 2^{n-2}(n-2)!(n-k-1) + (n-1-k) \left[ -A_{(n,k)} - (n-2-k) A_{(n-1,k)} \right] \\
 & + (n-1-k)(n-2-k) \left[ B_{(n,k)} + (n-3-k) B_{(n-1,k)} - B_{(n,k)} - (n-3-k) B_{(n-1,k)} \right] \\
 & = 2^{n-1}(n-1)! + 2^{n-2}(n-2)!(n-k-1) - (n-1-k) \left[ A_{(n,k)} + (n-2-k) A_{(n-1,k)} \right]
 \end{aligned}$$

On montre que  $A_{(n,k)} + (n-2-k) A_{(n-1,k)} = 2^{n-2}(n-2)!$  et le nombre de répétitions est donc  $2^{n-1}(n-1)!$  ce qui, en utilisant toutes les possibilités pour  $n$  et pour  $\lambda_{i_m}$  nous donne  $2^{t-1}(t-1)!$  répétitions.

. Enfin, calculons le nombre de répétitions d'un  $t$ -uplet constitué par les éléments des lignes d'ordre 1, 2, ...,  $t-1$  et  $t+1$ , éléments qui sont respectivement  $y_{i_1}, y_{i_2}, \dots, y_{i_{t-n}}, x_{i_{t-n+1}}, \dots$



...,  $x_{i_{t-1}}$  et  $y_i$ . On montre que, à  $n$  fixé et le choix  $\lambda_{i_m} = \gamma_{i_m}$  ou  $\theta_{i_m}$  étant fait pour les  $t-n$  composantes  $\in F$ , le  $t$ -uplet ne peut provenir que des  $2 \cdot \frac{(n-1)!}{(n-2)!}$   $t$ -uplets de  $T_E$  dont les éléments  $\lambda_{i_1}, \lambda_{i_2}, \dots, \lambda_{i_{t-n}}, x_{i_{t-n+1}}, \dots, x_{i_{t-1}}$  et  $\lambda_i$  se trouvent respectivement dans les lignes  $S_{\pi(1)}, S_{\pi(2)}, \dots$ , ...,  $S_{\pi(t-n)}, t-n+1, \dots, t-1$  et  $T_u$  pour  $T_u \in \{T_1, T_2, \dots, T_{n-1}\}$

On montre alors que le nombre de répétitions sera :

$$\frac{2(n-1)!}{(n-2)!} \left[ A_{(n,k)} - (n-2-k) B_{(n,k)} + \left( A_{(n-1,k)} - (n-3-k) B_{(n-1,k)} \right) (n-k-2) + B_{(n,k)} (n-k-2) + B_{(n-1,k)} (n-k-2)(n-k-3) \right]$$

Soit en tout  $\left[ A_{(n,k)} + (n-2-k) A_{(n-1,k)} \right] \cdot \frac{2(n-1)!}{(n-2)!} = 2^{n-1} (n-1)!$

qui, lorsque l'on épuise les possibilités pour  $\pi$  et pour  $\lambda_{i_m}$  donne bien  $2^{t-1} (t-1)!$  répétitions.

Théorème III.2.2. : Etant donné un tableau orthogonal  $(1, n+3, s_1, 2)$  et un tableau orthogonal  $(1, n+2, s_2, 2)$ , si  $s_1 > n s_2$ , il est possible de construire un tableau orthogonal  $(n, n+2, s_1 + s_2, 2)$  qui admet comme sous-tableau orthogonal  $(1, n+2, s_2, 2)$ .

Démonstration : Puisque  $s_1 > n s_2$ , il existe  $n$  ensembles  $\Gamma^{(i)}$  ( $i = 1, 2, \dots, n$ ) tels que  $\Gamma^{(i)} \subset E, \Gamma^{(i)} \cap \Gamma^{(j)} = \emptyset (i, j), i \neq j$   $\text{card} \Gamma^{(i)} = s_2$ ,  $E$  ensemble sur lequel est construit le tableau



orthogonal  $(1, n+3, s_1, 2)$ ,  $\text{card } E = s_1$ . Soit  $T_E$  le tableau orthogonal  $(1, n+3, s_1, 2)$ . Soit  $F$  l'ensemble sur lequel est construit le tableau orthogonal  $(1, n+2, s_2, 2)$  et soit  $T_F$  ce dernier tableau.

Soit  $E = \{x_i ; i = 1, 2, \dots, s_1\}$  soit  $F = \{y_i ; i = 1, 2, \dots, s_2\}$  et soit enfin  $\Gamma^{(i)} = \{\gamma_j^{(i)} ; j = 1, 2, \dots, s_2\} \quad \forall i = 1, 2, \dots, n$

Nous reprenons les notations de I.5 et la suite des colonnes de  $T_E$  est :

$(X, S(X), \Phi^{(1)}(X), \Phi^{(2)}(X), \dots, \Phi^{(n)}(X))$  où  $X$  décrit  $E^2$  et de la même façon la suite des colonnes de  $T_F$  est :

$(Y, \psi^{(1)}(Y), \psi^{(2)}(Y), \dots, \psi^{(n)}(Y))$  où  $Y$  décrit  $F^2$

Nous nous proposons de construire à partir de  $T_E$  et  $T_F$  un tableau orthogonal  $T_{EUF}$  sur  $E \cup F$ , tableau qui est constitué par :

1°) chacune des colonnes de  $T_F$  comptée  $n$  fois, ce qui nous donne en tout  $n(s_2)^2$  colonnes.

2°) soit  $Z$  le doublet constitué par le couple ordonné des éléments des 2 premières lignes. Si  $Z \in E \times F$  ou  $F \times E$ , par exemple :

$Z = (y_{i_1}, x_{i_2})$  nous mettrons dans  $T_{EUF}$  la colonne :

$(Z, \Phi^{(1)}(x_{j_1}, x_{i_2}), \Phi^{(2)}(x_{j_1}, x_{i_2}), \dots, \Phi^{(n)}(x_{j_1}, x_{i_2}))$

dans laquelle  $x_{j_1}$  est la solution unique de l'équation :

$$S(x_{j_1}, x_{i_2}) = \lambda_{i_1}$$

où  $\lambda_{i_1} = \gamma_{i_1}^{(1)}$  ou  $\gamma_{i_1}^{(2)}$  ou ..... ou  $\gamma_{i_1}^{(n)}$

ce dernier choix donne  $n$  possibilités, ce qui nous donne  $n s_2 s_1$  colonnes lorsque  $Z = (y_{i_1}, x_{i_2})$  et  $n s_2 s_1$  colonnes lorsque



$$Z = (x_{i_1}, y_{i_2})$$

3°) Si  $Z \in E^2$ , soit  $Z = (x_{i_1}, x_{i_2})$

a) si  $S(Z) \in \Gamma^{(i)}$ , soit  $S(Z) = \gamma_k^{(i)}$  alors nous mettrons

dans  $T_{EUF}$  les  $n$  colonnes suivantes :

$$\left( Z, \Phi^{(1)}(Z), \Phi^{(2)}(Z), \dots, \Phi^{(l-1)}(Z), y_k, \Phi^{(l+1)}(Z), \dots, \Phi^{(n)}(Z) \right) \\ , \forall l = 1, 2, \dots, n$$

b) si  $S(Z) \in \bigcap_{i=1}^n \overline{\Gamma}^{(i)}$  nous mettrons alors dans  $T_{EUF}$  la colonne :

$$\left( Z, \Phi^{(1)}(Z), \Phi^{(2)}(Z), \dots, \Phi^{(n)}(Z) \right) \text{ répétée } n \text{ fois.}$$

Or dans  $T_E$  il y a  $s_1^2 - n s_1 s_2$  colonnes telles que

$$S(Z) = S(X) \in \bigcap_{i=1}^n \overline{\Gamma}^{(i)}$$

le cas a) nous donne en x  $n s_1 s_2$  colonnes

le cas b) nous donne  $n(s_1^2 - n s_1 s_2)$  colonnes.

En tout on a obtenu un tableau  $T_{EUF}$  de  $n s_2^2 + 2 n s_2 s_1 + n^2 s_1 s_2 = n (s_1^2 - n s_1 s_2) = n (s_2 + s_1)^2$  colonnes. Prouvons que  $T_{EUF}$  est un tableau orthogonal  $(n, n+2, s_1+s_2, 2)$ .

1) la méthode de construction montre que si l'on considère les doublets constitués par les éléments de 2 premières lignes de  $T_{EUF}$ , ces doublets y sont tous et chacun est répété  $n$  fois.

2) Considérons les doublets constitués par un élément de la lère ligne et un élément de la  $(l+1)$ ème colonne ( $l = 1, 2, \dots, n$ )



- ceux de la forme  $(y_{i_1}, y_{i_{l+2}})$  y sont tous, chacun étant répété  $n$  fois à cause du fait que  $T_F$  est un tableau orthogonal  $(1, n+2, s_2, 2)$ .

- considérons ceux de la forme  $(y_{i_1}, x_{i_{l+2}})$  : un tel doublet ne peut provenir que de la colonne suivante de  $T_E$  (unique puisque  $T_E$  est un tableau orthogonal d'indice unité et de force 2) :

$$\left( x_{i_1}, x_{i_2}, \gamma_{i_1}^{(i)}, \Phi_{i_1}^{(1)}(x_{i_1}, x_{i_2}), \dots, \Phi_{i_1}^{(l-1)}(x_{i_1}, x_{i_2}), x_{i_{l+2}}, \Phi_{i_1}^{(l+1)}(x_{i_1}, x_{i_2}), \dots, \Phi_{i_1}^{(n)}(x_{i_1}, x_{i_2}) \right)$$

$i$  pouvant prendre  $n$  valeurs,  $(y_{i_1}, x_{i_{l+2}})$  se trouve bien dans  $T_{EUF}$  et ceci  $n$  fois

- considérons ceux de la forme  $(x_{i_1}, y_{i_{l+2}})$  : un tel doublet ne peut provenir que de la colonne suivante de  $T_E$  (unique puisque  $T_E$  est un tableau orthogonal d'indice unité et de force 2) :

$$\left( x_{i_1}, x_{i_2}, \gamma_{i_{l+2}}^{(i)}, \Phi_{i_{l+2}}^{(1)}(x_{i_1}, x_{i_2}), \Phi_{i_{l+2}}^{(2)}(x_{i_1}, x_{i_2}), \dots, \Phi_{i_{l+2}}^{(n)}(x_{i_1}, x_{i_2}) \right)$$

$i$  pouvant prendre  $n$  valeurs,  $(x_{i_1}, y_{i_{l+2}})$  se trouve bien dans  $T_{EUF}$  et ceci  $n$  fois.

- considérons enfin ceux de la forme  $(x_{i_1}, x_{i_{l+2}})$ . Soit alors  $x_{i_2}$  la solution unique de l'équation

$$\Phi_{i_1}^{(1)}(x_{i_1}, x_{i_2}) = x_{i_{l+2}}$$



a) si  $S(x_{i_1}, x_{i_2}) \in \bigcup_{i=1}^n \Gamma^{(i)}$ , le doublet peut se trouver dans la colonne de  $T_{EUF}$  telle que :

$$[x_{i_1}, y_{i_2}, x_{i_3}, \dots, x_{i_{l+2}}, \dots, x_{i_{n+2}}] \in E F E^n$$

il peut aussi se trouver dans les  $(n-1)$  colonnes :

$$[x_{i_1}, x_{i_2}, x_{i_3}, \dots, x_{i_{l+2}}, \dots, y_k, \dots, x_{i_{n+2}}] \in E^\mu F E^{n+1-\mu}$$

(il existe  $(n-1)$  telles colonnes ne différant entre elles que par la place de l'élément de  $F$  dans les lignes d'ordre 3, 4, ...,  $(l+1, l+3, \dots, n+2)$ ).

Dans ce cas le doublet  $(x_{i_1}, x_{i_{l+2}})$  se trouve donc dans  $n$  colonnes de  $T_{EUF}$ .

b) si  $S(x_{i_1}, x_{i_2}) \in \bigcap_{i=1}^n \overline{\Gamma}^{(i)}$  alors  $(x_{i_1}, x_{i_{l+2}})$  ne peut se trouver que dans la colonne suivante de  $T_{EUF}$  :

$$[x_{i_1}, x_{i_2}, x_{i_3}, \dots, x_{i_{l+2}}, \dots, x_{i_{n+2}}] \in E^{n+2}$$

laquelle colonne est répétée  $n$  fois dans  $T_{EUF}$ .

Dans ce cas encore  $(x_{i_1}, x_{i_{l+2}})$  se trouve donc dans  $n$  colonnes de  $T_{EUF}$ .

3°) considérons les doublets constitués par un élément de la  $(l+2)$ ème ligne et un élément de la  $(m+2)$ ème ligne ( $l \neq m$ )  
 $(l = 1, 2, \dots, n ; m = 1, 2, \dots, n)$

- ceux de la forme  $(y_{i_{l+2}}, y_{i_{m+2}})$  y sont tous, chacun étant répété  $n$  fois puisque  $T_F$  est un tableau orthogonal  
 $(1, n+2, s_2, 2)$ .



- considérons ceux de la forme  $(y_{i_{1+2}}, x_{i_{m+2}})$  : un tel doublet ne peut se trouver que dans une colonne de  $T_{EUF}$  telle que :

$$[x_{i_1}, x_{i_2}, x_{i_3}, \dots, y_{i_{1+2}}, \dots, x_{i_{m+2}}, \dots, x_{i_{n+2}}] \in E^{1+1} \times E^{n-1}$$

Or une telle colonne de  $T_{EUF}$  ne peut provenir que d'une colonne de  $T_E$  telle que :

$$[x_{i_1}, x_{i_2}, \gamma_{i_{1+2}}^{(i)}, \Phi^{(1)}(x_{i_1}, x_{i_2}), \dots, \Phi^{(m-1)}(x_{i_1}, x_{i_2}), x_{i_{m+2}}, \Phi^{(m+1)}(x_{i_1}, x_{i_2}), \dots, \Phi^{(n)}(x_{i_1}, x_{i_2})]$$

où  $(x_{i_1}, x_{i_2})$  est solution unique du système :

$$\begin{cases} S(x_{i_1}, x_{i_2}) = \gamma_{i_{1+2}}^{(i)} \\ \Phi^{(m)}(x_{i_1}, x_{i_2}) = x_{i_{m+2}} \end{cases}$$

Comme  $i$  peut prendre  $n$  valeurs, il existe bien dans  $T_{EUF}$  un doublet  $(y_{i_{1+2}}, x_{i_{m+2}})$  et ce doublet est répété  $n$  fois.

- considérons enfin ceux de la forme  $(x_{i_{1+2}}, x_{i_{m+2}})$

Soit  $(x_{i_1}, x_{i_2})$ , la solution (unique) du système :

$$\begin{cases} \Phi^{(1)}(x_{i_1}, x_{i_2}) = x_{i_{1+2}} \\ \Phi^{(m)}(x_{i_1}, x_{i_2}) = x_{i_{m+2}} \end{cases}$$

a) si  $S(x_{i_1}, x_{i_2}) \in \bigcup_{i=1}^n \Gamma^{(i)}$ , alors  $(x_{i_{1+2}}, x_{i_{m+2}})$  se trouve



$\alpha$ ) dans la colonne de  $T_{EUF}$  suivante :

$$[y_{i_1}, x_{i_2}, \dots, x_{i_{1+2}}, \dots, x_{i_{m+2}}, \dots, x_{i_{n+2}}] \in F E^{n+1}$$

$\beta$ ) dans la colonne de  $T_{EUF}$  suivante :

$$[x_{i_1}, y_{i_2}, \dots, x_{i_{1+2}}, \dots, x_{i_{m+2}}, \dots, x_{i_{n+2}}] \in E F E^n$$

$\gamma$ ) dans les  $(n-2)$  colonnes de  $T_{EUF}$  suivantes :

$$[x_{i_1}, x_{i_2}, \dots, y_k, \dots, x_{i_{1+2}}, \dots, x_{i_{m+2}}, \dots, x_{i_{n+2}}] \in E^\mu F E^{n+1-\mu}$$

(il y a  $(n-2)$  colonnes ne différant entre elles que par la place de l'élément de  $F$  dans les lignes d'ordre 3, 4, ...,  $1+1$ ,  $1+3$ , ...,  $m+1$ ,  $m+3$ , ...,  $n+2$ .)

Dans ce cas  $(x_{i_{1+2}}, x_{i_{m+2}})$  figure dans exactement  $n$  colonnes de  $T_{EUF}$ .

b) si  $S(x_{i_1}, x_{i_2}) \in \bigcap_{i=1}^n \overline{\Gamma^{(i)}}$ , alors  $(x_{i_{1+2}}, x_{i_{m+2}})$  ne peut se trouver que dans la colonne suivante de  $T_{EUF}$  :

$$[x_{i_1}, x_{i_2}, x_{i_3}, \dots, x_{i_{1+2}}, \dots, x_{i_{m+2}}, \dots, x_{i_{n+2}}] \in E^{n+2}$$

laquelle colonne est répétée  $n$  fois dans  $T_{EUF}$ .

Dans ce cas encore  $(x_{i_{1+2}}, x_{i_{m+2}})$  se trouve donc dans exactement  $n$  colonnes de  $T_{EUF}$ .

Le théorème III.2.2. permet pour  $n = 2$ ,  $s_1 > 2 s_2$ , de construire à partir de 2 tableaux orthogonaux  $(1, 5, s_1, 2)$  et  $(1, 4, s_2, 2)$ , un tableau orthogonal  $(2, 4, s_1+s_2, 2)$ . Nous allons voir que si d'autres conditions sont réalisées, on peut



aboutir à la construction d'un tableau orthogonal  $(1, 4, s_1 + s_2, 2)$ . C'est la méthode utilisée par Yamamoto pour construire des quasi-groupes mutuellement orthogonaux. Le principe de la méthode de Yamamoto est le même que celui des méthodes de construction de tableaux orthogonaux exposées dans les démonstrations des Théorèmes III.2.1 et III.2.2.

Nous reprenons donc les notations du Théorème III.2.2, pour  $n = 2$ . Nous appelons  $\sigma^{(1)}$ ,  $\tau^{(1)}$ ,  $\sigma^{(2)}$ ,  $\tau^{(2)}$  quatre permutations de l'ensemble  $\{1, 2, \dots, s_2\}$ .

Nous construisons un tableau  $T_{EUF}$  de la façon suivante :

1°) nous mettons chacune des colonnes de  $T_F$

2°) si  $Z = (x_{i_1}, y_{i_2}) \in E \times F$ , nous mettons dans  $T_{EUF}$  la colonne :

$$\left[ Z, \Phi^{(1)}(x_{i_1}, x_{j_2}), \Phi^{(2)}(x_{i_1}, x_{j'_2}) \right]$$

$$\text{où } x_{j_2} \text{ est tel que } S(x_{i_1}, x_{j_2}) = \bigvee^{(1)} \sigma^{(1)}(i_2)$$

$$\text{et } x_{j'_2} \text{ est tel que } S(x_{i_1}, x_{j'_2}) = \bigvee^{(2)} \sigma^{(2)}(i_2)$$

3°) si  $Z = (y_{i_1}, x_{i_2}) \in F \times E$ , nous mettons dans  $T_{EUF}$  la

$$\text{colonne : } \left[ Z, \Phi^{(1)}(x_{j_1}, x_{i_2}), \Phi^{(2)}(x_{j'_1}, x_{i_2}) \right]$$

$$\text{où } x_{j_1} \text{ est tel que } S(x_{j_1}, x_{i_2}) = \bigvee^{(1)} \tau^{(1)}(i_1)$$

$$\text{et } x_{j'_1} \text{ est tel que } S(x_{j'_1}, x_{i_2}) = \bigvee^{(2)} \tau^{(2)}(i_1)$$



4°) si  $Z = (x_{i_1}, x_{i_2}) \in E^2$

a) si  $S(x_{i_1}, x_{i_2}) = \gamma_j^{(1)}$ , alors on met la colonne

$$[Z, y_j, \Phi^{(2)}(x_{i_1}, x_{i_2})]$$

b) si  $S(x_{i_1}, x_{i_2}) = \gamma_j^{(2)}$ , alors on met la colonne

$$[Z, \Phi^{(1)}(x_{i_1}, x_{i_2}), y_j]$$

c) si  $S(x_{i_1}, x_{i_2}) \in \bigcap_{i=1}^2 \overline{\Gamma}^{(i)}$ , alors on met la colonne

$$[Z, \Phi^{(1)}(x_{i_1}, x_{i_2}), \Phi^{(2)}(x_{i_1}, x_{i_2})]$$

L'examen du tableau  $T_{EUF}$  ainsi formé, qui possède  $(s_1 + s_2)^2$  colonnes, montre que ce tableau n'est un tableau orthogonal  $(1, 4, S_1 + S_2, 2)$  que si la condition

$A^{(1)} \cup A^{(2)} = B^{(1)} \cup B^{(2)}$  est réalisée, où

$$A^{(1)} = \left\{ \left( \Phi^{(1)}(x_i, x_j), \Phi^{(2)}(x_i, x_j) \right) \mid S(x_i, x_j) = \gamma_t^{(1)} ; \forall t=1, 2, \dots, s_2 \right\}$$

$$A^{(2)} = \left\{ \left( \Phi^{(1)}(x_i, x_j), \Phi^{(2)}(x_i, x_j) \right) \mid S(x_i, x_j) = \gamma_t^{(2)} ; \forall t=1, 2, \dots, s_2 \right\}$$

$$B^{(1)} = \left\{ \left( \Phi^{(1)}(x_i, x_j), \Phi^{(2)}(x_i, x_k) \right) \mid S(x_i, x_j) = \gamma_{\sigma(1)(t)}^{(1)} \text{ et } \right.$$

$$S(x_i, x_k) = \gamma_{\sigma(2)(t)}^{(2)} ; \forall t=1, 2, \dots, s_2$$

$$B^{(2)} = \left\{ \left( \Phi^{(1)}(x_i, x_j), \Phi^{(2)}(x_k, x_j) \right) \mid S(x_i, x_j) = \gamma_{\tau(1)(t)}^{(1)} \text{ et } \right.$$

$$S(x_k, x_j) = \gamma_{\tau(2)(t)}^{(2)} ; \forall t=1, 2, \dots, s_2 \left. \right\}$$



Théorème III.2.3 : S'il existe un tableau orthogonal  $T_F(1,4,s_2,2)$  construit sur  $F$  et un tableau orthogonal  $T_E(1,5,s_1,2)$  construit sur  $E$  :

$T_E = \{ [x_i, x_j, S(x_i, x_j), \Phi^{(1)}(x_i, x_j), \Phi^{(2)}(x_i, x_j)] ; \forall (x_i, x_j) \in E^2 \}$ ,  
 Si  $s_1 > 2$   $s_2$  et s'il existe  $\Gamma^{(1)} \subset E, \Gamma^{(2)} \subset E \mid \Gamma^{(1)} \cap \Gamma^{(2)} = \emptyset$   
 et  $\text{card } \Gamma^{(1)} = \text{card } \Gamma^{(2)} = s_2$ , ainsi que 2 permutations  $\sigma^{(1)}$  et  $\tau^{(1)}$  des éléments  $\gamma_t^{(1)}$  de  $\Gamma^{(1)}$  et 2 permutations  $\sigma^{(2)}$  et  $\tau^{(2)}$  des éléments  $\gamma_t^{(2)}$  de  $\Gamma^{(2)}$  répondant à la condition  
 $A^{(1)} \cup A^{(2)} = B^{(1)} \cup B^{(2)}$ , (les ensembles  $A^{(1)}, A^{(2)}, B^{(1)}, B^{(2)}$  ayant été précédemment définis), alors on peut construire sur  $E \cup F$  un tableau orthogonal  $T_{EUF}(1, 4, s_1+s_2, 2)$ .  $T_{EUF}$  admet alors  $T_F$  comme sous-tableau.

Remarque : cas où  $T_E$  est construit sur un anneau commutatif possédant un élément unité :

On suppose que  $E(+, \cdot)$  est un anneau commutatif possédant un élément unité.  $T_E$  est défini par :

$$S(x_i, x_j) = x_i - x_j$$

$$\Phi^{(1)}(x_i, x_j) = \alpha_1 x_i + \beta_1 x_j$$

$$\Phi^{(2)}(x_i, x_j) = \alpha_2 x_i + \beta_2 x_j$$

Pour que  $T_E$  soit un tableau orthogonal, il faut et il suffit que :

1°)  $\alpha_1, \beta_1, \alpha_2, \beta_2$  soient réguliers :  $(x_i, \Phi^{(k)}(x_i, x_j))$  balaie alors  $E^2$  lorsque  $(x_i, x_j)$  balaie  $E^2$  ( $1 = i, j ; k = 1, 2$ ).



2°)  $\alpha_1 + \beta_1$  et  $\alpha_2 + \beta_2$  soient réguliers :  $(\Phi^{(k)}(x_i, x_j), S(x_i, x_j))$  balaie alors  $E^2$  lorsque  $(x_i, x_j)$  balaie  $E^2$ . ( $k = 1, 2$ )

3°)  $\alpha_1 \beta_2 - \alpha_2 \beta_1$  soit régulier :  $(\Phi^{(1)}(x_i, x_j), \Phi^{(2)}(x_i, x_j))$  balaie alors  $E^2$  lorsque  $(x_i, x_j)$  balaie  $E^2$ .

La condition  $A^{(1)} \cup A^{(2)} = B^{(1)} \cup B^{(2)}$  se transforme alors en la condition

$$\Gamma^{(1)} \cup \Gamma^{(2)} = H^{(1)} \cup H^{(2)}$$

où  $H^{(1)}$  et  $H^{(2)}$  sont définis de la façon suivante :

$$H^{(1)} = \left\{ \left( \lambda \gamma_{\sigma^{(2)}(t)}^{(2)} + (1 - \lambda) \gamma_{\sigma^{(1)}(t)}^{(1)} \right), \forall t = 1, 2, \dots, s_2 \right\}$$

$$H^{(2)} = \left\{ \left( \varepsilon \gamma_{\tau^{(1)}(t)}^{(1)} + (1 - \varepsilon) \gamma_{\tau^{(2)}(t)}^{(2)} \right), \forall t = 1, 2, \dots, s_2 \right\}$$

$$\text{avec } \lambda = \frac{\beta_2 + (\alpha_1 + \beta_1)}{\alpha_1 \beta_2 - \alpha_2 \beta_1}, \quad \varepsilon = \frac{\alpha_1 (\alpha_2 + \beta_2)}{\alpha_1 \beta_2 - \alpha_2 \beta_1}$$

### III.3 - Construction de tableaux orthogonaux par la méthode de

Sade étendue aux tableaux orthogonaux de force quelconque : [XV] et [XIX]

Soient les ensembles,  $E, F \subset E, G = \begin{pmatrix} F \\ E \end{pmatrix}$ , tels que

$\text{card } E = m, \text{ card } F = p < m$ , et  $H$  tel que  $\text{card } H = h$ , nous nous plaçons dans les hypothèses suivantes :

- 1) Il existe un tableau orthogonal  $T_E(1, r+t, m, t)$
- 2) Le tableau orthogonal  $T_E(1, r+t, m, t)$  admet un sous-tableau orthogonal construit sur F, soit  $T_F(1, r+t, p, t)$ .



- 3) Il existe, construit sur  $G = \begin{pmatrix} F \\ E \end{pmatrix}$ , un tableau orthogonal  $T_G(1, r+2t-2, m-p, t)$ .
- 4) Il existe un tableau orthogonal construit sur  $H$ , soit  $T_H(1, r+t, h, t)$  et ce tableau admet un sous-tableau orthogonal  $T_{H_{t-1}}(1, r+t, h, t-1)$  construit sur le même ensemble  $H$ , et  $T_{H_{t-1}}$  admet un sous-tableau orthogonal  $T_{H_{t-2}}(1, r+t, h, t-2)$  construit sur le même ensemble  $H$  etc....., et  $T_{H_1}$  admet un sous-tableau orthogonal  $T_{H_{1-1}}(1, r+t, h, 1-1)$ , ....., et  $T_{H_2}$  admet un sous-tableau orthogonal  $T_{H_1}(1, r+t, h, 1)$ .

Nous remarquons que s'il existe, construit sur  $H$ , un tableau orthogonal  $T_H(1, r+2t-1, h, t)$ , alors l'hypothèse (4) est vérifiée. en vertu du Théorème du paragraphe I.11.

Les hypothèses (1) et (2) entraînent l'inégalité :  $m - p \geq r p$ , pour  $t \geq 2$ , en vertu du 1er théorème du paragraphe I.13. Il en résulte que l'on peut trouver une famille de parties  $G_i$  ( $i = 1, 2, \dots, r$ ) deux à deux disjointes de  $G$  telles que  $\text{card } G_i = p$ .

Soit  $\rho_i$  une application bijective de  $F$  sur  $G_i$  ( $i = 1, 2, \dots, r$ ). Un tableau orthogonal d'indice unité étant considéré comme ensemble de ses colonnes, on notera :

$H^{(1)}$  le tableau  $T_{H_1}(1, r+t, h, 1)$

$H^{(2)}$  le complément de  $T_{H_1}(1, r+t, h, 1)$  dans  $T_{H_2}(1, r+t, h, 2)$

.....

$H^{(1)}$  le complément de  $T_{H_{1-1}}(1, r+t, h, 1-1)$  dans  $T_{H_1}(1, r+t, h, 1)$



.....  
 $H^{(t)}$  le complément de  $T_{H_{t-1}}(1, r+t, h, t-1)$  dans  $T_H(1, r+t, h, t)$

L'ensemble  $\{H^{(j)}, j = 1, 2, \dots, t\}$  constitue alors une partition de  $T_H(1, r+t, h, t)$ .

On utilisera les notations suivantes :

$$T_E = \left\{ [X] = (X, E_1(X), E_2(X), \dots, E_r(X)) ; \forall X \in E^t \right\}$$

où  $E_u(X)$  est l'élément de la  $(t+u)$ ème ligne de la colonne  $[X]$  considérée, et de la même façon :

$$T_F = \left\{ [X'] = (X', F_1(X'), F_2(X'), \dots, F_r(X')) ; \forall X' \in F^t \right\}$$

$$T_G = \left\{ [X''] = (G_1(X''), G_2(X''), \dots, G_{t-2}(X''), X'', G_{2t-1}(X''), \dots, \dots, G_{2t-2+r}(X'')) ; \forall X'' \in G^t \right\}$$

$$T_H = \left\{ [Y] = (Y, H_1(Y), H_2(Y), \dots, H_r(Y)) ; \forall Y \in H^t \right\}$$

et enfin le tableau  $T_F \cup (G \times H)$  que nous proposons de construire sur  $F \cup (G \times H)$  sera la juxtaposition de colonnes :

$$[Z] = (Z, \xi_1(Z), \xi_2(Z), \dots, \xi_r(Z)) , \text{ où } Z \text{ est un}$$

$t$ -uple dont  $t-k$  composantes appartiennent à  $F$  et  $k$  composantes appartiennent à  $G \times H$  ( $k = 0, 1, 2, \dots, t$ ).

A  $Z$  on associera  $X$  obtenu en projetant sur  $G$  chaque composante de  $Z$  appartenant à  $G \times H$ , ainsi que  $Y$  obtenu de la façon suivante ; si  $Z$  a  $k$  composantes appartenant à  $G \times H$  et si ces composantes sont celles de rang  $i_1, i_2, \dots, i_k$ , on cherche dans  $T_{H_k}$  la colonne  $[Y]$  dont les  $k$  composantes de rang  $i_1, i_2, \dots, i_k$  sont celles obtenues en projetant respectivement les composantes de  $Z$  de rang  $i_1, i_2, \dots, i_k$  sur  $H$ .  $Y$  est déterminé de façon



unique en vertu de l'hypothèse (4).

On envisage successivement les cas suivants :

1°)  $k = 0$  : on construit alors la colonne  $[Z]$  telle que

$$\xi_u(Z) = E_u(X) \quad (u = 1, 2, \dots, r)$$

car alors  $E_u(X) \in F$ . On met dans  $T_F U(G \times H)$  cette colonne répétée  $r^{t-2}(t-2)!$  fois et l'on obtient ainsi  $(t-2)! r^{t-2} p^t$  colonnes.

2°)  $k = 1$  : on construit la colonne  $[Z]$  telle que

$$\xi_u(Z) = (E_u(X), H_u(Y)) \quad (u = 1, 2, \dots, r)$$

car alors,  $(2) \Rightarrow E_u(X) \in G \quad (u = 1, 2, \dots, r)$ . On met dans  $T_F U(G \times H)$  cette colonne répétée  $r^{t-2}(t-2)!$  fois, et l'on obtient ainsi  $C_t^1 p^{t-1} (m-p) h(t-2)! r^{t-2}$  colonnes

3°)  $k \notin \{0, 1\}$  :

a) si  $[Y] \in H^{(1)}$ , alors le  $r$ -uplet  $(E_1(X), E_2(X), \dots, E_r(X))$

a  $(k-v)$  composantes appartenant à  $F$  et  $(r-k+v)$  composantes appartenant à  $G$ , avec  $v = 1$  ou  $2$  ou .... ou  $k$ .

Supposons que  $E_u(X) \in F, \forall u \in \{\alpha_1, \alpha_2, \dots, \alpha_{k-v}\}$

et  $E_u(X) \in G, \forall u \notin \{\alpha_1, \alpha_2, \dots, \alpha_{k-v}\}$

On construit alors  $[Z]$  telle que :

$$\xi_u(Z) = E_u(X), \quad \forall u \in \{\alpha_1, \alpha_2, \dots, \alpha_{k-v}\}$$

$$\xi_u(Z) = (E_u(X), H_u(Y)), \quad \forall u \notin \{\alpha_1, \alpha_2, \dots, \alpha_{k-v}\}$$

on répète chaque colonne ainsi construite  $r^{t-2}(t-2)!$  fois et l'on obtient ainsi  $C_t^k p^{t-k} (m-p)^k h r^{t-2}(t-2)!$  colonnes.



b) si  $[Y] \in H^{(1)}$  ( $1 = 2, 3, \dots, k$ ), soit  $B = \{\beta_1, \beta_2, \dots, \beta_{t-k}\}$

l'ensemble des numéros des lignes de  $Z$  contenant les éléments de  $F$  et soit  $C = \{\gamma_1, \gamma_2, \dots, \gamma_k\}$  l'ensemble des numéros des lignes de  $Z$  contenant les éléments de  $G \times H$ .

Soit  $x'_{\beta_\mu}$  l'élément de la ligne  $\beta_\mu$  de  $Z$  et soit  $(x''_{\gamma_\nu}, y_{\gamma_\nu})$

l'élément de la ligne  $\gamma_\nu$ . Soit  $\pi$  une application injective de  $B$  dans  $\{1, 2, \dots, t-2\}$  et soit  $\sigma$  une application de  $B$  dans  $\{1, 2, \dots, r\}$ . On détermine la colonne  $[X'']$  de  $T_G$  par les conditions :

$\rho_{\sigma(\beta_\mu)}(x'_{\beta_\mu})$  est la composante de rang  $\pi(\beta_\mu)$ ,  $\forall \mu \in \{1, 2, \dots, t-k\}$

$x''_{\gamma_\nu}$  est la composante de rang  $t-2+\gamma_\nu$ ,  $\forall \nu \in \{1, 2, \dots, k\}$

Parmi les  $(t-2)$  premières lignes de  $[X'']$  il y en a  $(k-2)$  de rang différent de  $\pi(\beta_\mu)$ .

Supposons que parmi les éléments de ces  $(k-2)$  lignes, il y en ait  $(k-1-c+d)$  qui appartiennent à  $\bigcup_{i=1}^r \mathcal{G}_i$ , soit  $x''_{\delta_\omega} \in \mathcal{G}_{i_{\delta_\omega}}$

pour  $\omega = 1, 2, \dots, (k-1-c+d)$  ( $c \geq k-1-r$ )

Soit  $\mathcal{E} = \{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{k-1-c}\} \subset \{\delta_1, \delta_2, \dots, \delta_{k-1-c+d}\} = \mathcal{S}$

Soit  $\tau$  une application injective de  $\mathcal{E}$  dans  $R = \{2t-1, 2t, \dots, 2t-2+r\}$

On construira la colonne  $[Z]$  telle que :

$$\sum \tau(\varepsilon_a) - 2t + 2 (Z) = \rho_i^{-1} (x''_{\varepsilon_a}) \quad (a = 1, 2, \dots, k-1-c)$$

$$\sum_u (Z) = (G_{2t-2+u}(X''), H_u(Y)) \text{ pour } u \text{ tel que } 2t-2+u \in \left( \tau(\mathcal{E}) \right)_R$$



- si  $d-c > 0$ ,  $\sup(0, k-1-r) \leq c \leq k-1$  et l'on répète chaque colonne ainsi obtenue

$$d! \sum_{w=0}^{w=c} (-1)^w \frac{r^{1+c-2-w} (1+c-2-w)!}{(d-w)!} C_{r+w-1}^w \text{ fois}$$

- si  $d-c \leq 0$ ,  $0 \leq k-1-c \leq \inf(k-1-c+d, r)$  et l'on répète la colonne ainsi obtenue

$$d! \sum_{w=0}^{w=d} (-1)^w \frac{r^{1+c-2-w} (1+c-2-w)!}{(d-w)!} C_{r+w-1}^w \text{ fois}$$

Enfin on construit autant de colonnes qu'il y a de possibilités dans le choix de  $\tau$ , de  $\sigma$  et de  $\tau$ .

Si  $d-c = D > 0$ , si  $k-1-r \leq 0$ , on obtient dans ces conditions :

$$\frac{(t-2)!}{(k-2)!} r^{t-k} \sum_{c=0}^{k-1} \frac{r! d! (k-1-c+d)!}{(r-k+1+c)! (k-1-c)! d!} \sum_{w=0}^c (-1)^w C_{r+w-1}^w \frac{(1+c-2-w)! r^{1+c-2-w}}{(d-w)!}$$

colonnes, quantité qui se met sous la forme :

$$\frac{(t-2)!}{(k-2)!} r^{t-k} \sum_{u=0}^{k-1} \frac{(k-1+D)! (1+u-2)!}{(D+u)!} r^{1+u-2} \sum_{w=0}^{k-1-u} (-1)^w C_{r+w-1}^w C_r^{k-1-u-w}$$

$$\text{Or } \sum_{w=0}^{k-1-u} (-1)^w C_{r+w-1}^w C_r^{k-1-u-w} = 0 \text{ sauf pour } u = k-1$$

$$\text{où } \sum_{w=0}^{k-1-u} (-1)^w C_{r+w-1}^w C_r^{k-1-u-w} = 1$$

Le nombre de colonnes obtenues est donc :

$$\frac{(t-2)!}{(k-2)!} r^{t-k} \frac{(k-1+D)! (1+k-1-2)! r^{1+k-1-2}}{(D+k-1)} = (t-2)! r^{t-2} \text{ colonnes}$$



On montrerait que dans tous les autres cas il correspond bien à  $[Z] (t-2)! r^{t-2}$  colonnes. On obtient donc ainsi en tout :

$$C_t^k p^{t-k} (m-p)^k (h^1 - h^{1-1}) (t-2)! r^{t-2} \text{ colonnes}$$

et lorsque l prend toutes les valeurs possibles et k toutes les valeurs possibles, le tableau  $T_{FU(G \times H)}$  ainsi construit sera composé de

$$(p + (m-p)h)^t (t-2)! r^{t-2} \text{ colonnes.}$$

Théorème III.3.1 : Dans les hypothèses (1), (2), (3), (4), décrites ci-dessus, le tableau  $T_{FU(G \times H)}$  construit par la méthode que l'on vient d'exposer est un tableau orthogonal  $((t-2)! r^{t-2}, t+r, p+(m-p)h, t)$ . et  $T_{FU(G \times H)}$  contient  $T_F(1, t+r, p, t)$  comme sous-tableau orthogonal.

Démonstration : Soit  $T \in [FU(G \times H)]^t$ , supposons que k de ses composantes appartiennent à  $G \times H$  et  $(t-k)$  de ses composantes appartiennent à F. Nous faisons alors correspondre à T,  $U \in (FUG)^t = E^t$  obtenu en laissant intactes les composantes appartenant à F et en remplaçant celles qui appartiennent à  $G \times H$  par leur projection sur G. Nous faisons aussi correspondre à T,  $V \in H^k$  obtenu en supprimant les composantes appartenant à F et en remplaçant celles qui appartiennent à  $G \times H$  par leur projection sur H. Nous cherchons le nombre de répétitions de T fixé dans  $T_{FU(G \times H)}$  lorsque la même composante de T se trouve dans la ligne  $i_n$  de  $T_{FU(G \times H)}$ .

Nous devons montrer que ce nombre de répétitions est  $r^{t-2}(t-2)!$  Avant d'envisager les différents cas qui se présentent, nous remarquons qu'étant donné  $Z \in (FUG \times H)^t$ , dont  $(t-k)$  composantes exactement appartiennent à F, si  $[Y] \in H^{(1)}$  la construction utilise  $T_E$  et alors parmi les r dernières lignes d'une colonne correspondant à Z  $(k-1)$  composantes au plus peuvent appartenir à F, et si  $[Y] \in H^{(1)} \quad (1 \neq 1)$ , la construction utilise  $T_G$  et alors parmi les r dernières lignes d'une colonne correspondant à Z  $(k-2)$  composantes au plus peuvent appartenir à F.



1°) si  $k = 0$ ,  $T$  ne peut provenir que de  $T_F$  et est alors répété  $r^{t-2}(t-2)!$  fois, comme chaque colonne de  $T_F$  dans  $T_{FU}(G \times H)$

2°) si  $k = 1$ , supposons que parmi les  $(t-1)$  composantes qui appartiennent à  $F$ ,  $t-k'$  se trouvent dans les  $t$  premières lignes de  $T_{FU}(G \times H)$  et  $(k'-1)$  les  $r$  dernières. D'après la remarque que nous venons de faire  $U$  ne peut provenir que de  $T_E$ . Or dans la partie de  $T_E$  utilisée se trouvent tous les  $t$ -uples tels que  $U$  une fois et une seule ( $T_E$  est un tableau orthogonal de force  $t$ ). De plus  $H^{(1)}$  est un tableau orthogonal de force 1 et donc  $T$  fixé se trouve bien dans  $T_{FU}(G \times H)$  et est répété  $r^{t-2}(t-2)!$  fois.

3°) si  $k \notin \{0, 1\}$ , supposons que les composantes de  $T$  qui appartiennent à  $F$  se trouvent dans les lignes  $i'_1, i'_2, \dots, i'_{t-k}$  de  $T_{FU}(G \times H)$  et que celles qui appartiennent à  $G \times H$  se trouvent dans les lignes  $i''_1, i''_2, \dots, i''_k$  de  $T_{FU}(G \times H)$ . Supposons que

$$\{i'_{a_1}, i'_{a_2}, \dots, i'_{a_{t-k-u}}\} \subset \{1, 2, \dots, t\}$$

$$\{i''_{b_1}, i''_{b_2}, \dots, i''_{b_{k-v}}\} \subset \{1, 2, \dots, t\}$$

$V$  détermine dans  $T_{H_k}$  une colonne  $[V]$  de la façon suivante :

la composante de rang  $c$  de  $V$  ( $c = 1, 2, \dots, k$ ) doit se trouver dans la ligne  $i''_c$  de  $T_{H_k}$ . (la détermination de  $V$  est unique puisque  $T_{H_k}$  est un tableau orthogonal de force  $k$  et d'indice unité).

a) si  $[V] \in H^{(1)}$  : la méthode de construction montre que seul  $T_E$  a été utilisé ; dans  $T_E$  se trouvent tous les  $t$ -uples  $T$ , dont les composantes figurent à une place donnée, une fois et une seule. Comme dans ce cas on a répété les colonnes de  $T_E$   $r^{t-2}(t-2)!$  fois, le  $t$ -uple particulier  $T$  est bien répété exactement  $r^{t-2}(t-2)!$  fois.



b) si  $[V] \in H^{(1)}$  ( $1 \neq 1$ ) : la méthode de construction montre que seule  $T_G$  a été utilisé. On sait que les éléments de  $F$  proviennent des  $(t-2)$  premières lignes de  $T_G$ . Supposons que pour ces éléments de  $F$  le choix des  $Q_i$  soit fait, que le choix de  $\pi$  soit fait pour les  $(t-k-u)$  composantes de  $F$  telles que l'ensemble des numéros des lignes occupées par ces éléments est  $\{i'_{a_1}, i'_{a_2}, \dots, i'_{a_{t-k-u}}\}$ , et que le choix de  $\tau$  soit fait. Supposons donc que la colonne de  $T_G$  ainsi déterminée à partir de  $T$  soit telle que parmi les  $(t-2)$  premières composantes, figurent  $\lambda$  éléments  $\bigcup_{i=1}^r Q_i$ , en plus des  $t-k$  éléments qui ont servi à déterminer cette colonne.

Alors  $T$  pourra provenir d'un  $Z$  tel que  $(t-k-u+j)$  de ses composantes appartiennent à  $F$  et  $(k+u-j)$ , de ses composantes appartiennent à  $G \times H$ . ( $0 \leq j \leq \lambda$ ) et ne pourra provenir que de tels  $Z$ , et cela de

$$\frac{\lambda!}{(\lambda-j)! j!} \cdot \frac{(u+v)!}{(u+v-j)!} \text{ façons. Dans ces}$$

conditions le nombre de répétitions de  $T$  sera :

$$\begin{aligned} & \frac{(\lambda, u+v)}{j=0} \frac{\lambda!}{(\lambda-j)! j!} \frac{(u+v)!}{(u+v-j)!} \sum_{i=0}^{\inf(\lambda-j, r-u-v)} \frac{(\lambda-j)!(r-u-v)!(\lambda-i-j)!}{i!(\lambda-j-i)!(r-u-v-i)!} \\ & \sum_{w=0}^{\inf(\lambda-i, k-j-i-1)} (-1)^w \frac{r^{k-j-i-2-w} (k-j-i-2-w)!}{(\lambda-i-j-w)!} C_{r+w-1}^w \\ & = \sum_{j=0}^{\lambda} \sum_{i=0}^{\lambda-j} \sum_{w=0}^{\lambda-i-j} (-1)^w \frac{\lambda! (u+v)! (r-u-v)! r^{k-j-i-2-w} (k-j-i-2-w)!}{j! (u+v-j)! i! (r-u-v-i)! (\lambda-i-j-w)!} C_{r+w-1}^w \end{aligned}$$

en convenant que la présence de  $a!$ , avec  $a < 0$  dans cette expression annule le terme correspondant. Ce nombre de répétitions peut être mis sous la forme suivante en posant  $z = i+j$ .



$$\begin{aligned}
& \sum_{w=0}^{\lambda} \sum_{z=0}^{\lambda-w} (-1)^w \frac{r^{k-z-2-w} (k-z-2-w)! \lambda! C_{r+w-1}^w}{(\lambda-z-w)!} \sum_{i=0}^z C_{u+v}^{z-i} C_{r-u-v}^i \\
= & \sum_{w=0}^{\lambda} \sum_{z=0}^{\lambda-w} (-1)^w C_{r+w-1}^w C_r^z \frac{r^{k-z-2-w} (k-z-2-w)! \lambda!}{(\lambda-z-w)!}
\end{aligned}$$

En posant  $z' = z+w$ , ce nombre devient :

$$\sum_{z'=0}^{\lambda} \frac{\lambda! r^{k-z'-2} (k-z'-2)!}{(\lambda-z')!} \sum_{w=0}^{z'} (-1)^w C_{r+w-1}^w C_r^{z'-w}$$

or  $\sum_{w=0}^{z'} (-1)^w C_{r+w-1}^w C_r^{z'-w} = 0$  ,  $\forall z' \neq 0$ , on obtient donc

$$\lambda! \frac{r^{k-2} (k-2)!}{\lambda!} = r^{k-2} (k-2)!$$

Le choix de  $Q_i$  nous donne  $r^{t-k}$  possibilités.

Le choix de  $\eta$  et  $\tau$  en donne  $\frac{(t-2)!}{(k-2)!}$ .

T est donc bien répété en tout  $r^{t-2} (t-2)!$  fois.



# IV - RESULTATS SUR

## L'EXISTENCE DES TABLEAUX ORTHOGONAUX

Puisque l'existence d'un tableau orthogonal  $(\lambda, r, S, t)$  entraîne celle d'un tableau orthogonal  $(\lambda, r_1, S, t)$  pour  $r_1 < r$  (il suffit de supprimer  $r - r_1$  lignes du tableau orthogonal  $(\lambda, r, S, t)$ ), la non-existence d'un tableau orthogonal  $(\lambda, r, S, t)$ , entraîne la non-existence d'un tableau orthogonal  $(\lambda, r, S, t)$  avec  $r > r_1$ . Il suffira donc de prouver qu'il n'existe pas de tableau orthogonal  $(\lambda, r_1, S, t)$  pour prouver que le nombre maximum de contraintes d'un tableau orthogonal de force  $t$ , construit sur un ensemble de  $S$  éléments, et d'indice  $\lambda$  est inférieur ou égal à  $r_1 - 1$ . Dans ce chapitre nous noterons  $f(\lambda, S, t)$  le nombre maximum de contraintes d'un tel tableau orthogonal.

### IV.1 - Tableaux orthogonaux d'indice unité : [V]

#### Théorème IV.1.1. :

Si  $S \leq t$ , alors  $f(1, S, t) = t + 1$

Démonstration : Soit  $E = \{0, 1, 2, \dots, S-1\}$  l'ensemble sur lequel est construit un tableau orthogonal de force  $t$  et possédant  $t+2$  lignes ( $S \leq t$ ). Par isotopie, on peut se ramener à un tableau orthogonal dont la première colonne ne contient que l'élément 0. Nous distinguons les 3 cas suivants :

1°)  $S = 2$  : Soit  $a_{ij}$  l'élément de la  $i$ ème ligne et de la  $j$ ème colonne. Nous supposons donc que  $a_{i1} = 0, \forall i = 1, 2, \dots, t+2$ . Nous pouvons supposer que  $a_{i2} = 0, \forall i = 4, 5, \dots, t+2$ , que  $a_{43} = a_{44} = 1, a_{i3} = 0, \forall i = 5, 6, \dots, t+2$ , et enfin  $a_{i4} = 0, \forall i = 5, 6, \dots, t+2$ . On en déduit que :



$a_{i2} = 1$  pour  $i = 1, 2, 3$ , car s'il n'en était pas ainsi les 2 premières colonnes auraient 2 t-uples identiques (formés uniquement de 0). D'autre part, la 3ème colonne a  $(t-2)$  éléments en commun avec chacune des 2 premières. Elle peut donc avoir au plus un élément en commun avec une de ces colonnes dans les 3 premières lignes. Cela est impossible car on doit alors remplir 3 lignes avec 2 éléments 0 ou 1 et que chacun de ces 2 éléments ne devrait servir qu'une fois.

2°) S = 3 : Soit  $a_{ij}$  l'élément de la  $i$ ème ligne et de la  $j$ ème colonne. Nous pouvons supposer :

$$\begin{aligned}
 a_{i1} &= 0 \quad \forall i = 1, 2, \dots, t+2 \\
 a_{i2} &= 0 \quad \forall i = 4, 5, \dots, t+2 ; \text{ avec } a_{i2} \neq 0 \text{ pour } i = 1, 2, 3 \\
 a_{i3} &= 0 \quad \forall i = 4, 5, \dots, t+2 ; \text{ avec } a_{i3} \neq 0 \text{ pour } i = 1, 2, 3 \\
 a_{i4} &= 0 \quad \forall i = 1, 5, 6, \dots, t+2 ; a_{44} = 1 ; a_{i4} \neq 0 \text{ pour } i = 2, 3 \\
 a_{i5} &= 0 \quad \forall i = 2, 5, 6, \dots, t+2 ; a_{45} = 1 ; a_{i5} \neq 0 \text{ pour } i = 1, 3 \\
 a_{i6} &= 0 \quad \forall i = 3, 5, 6, \dots, t+2 ; a_{46} = 1 ; a_{i6} \neq 0 \text{ pour } i = 1, 2 \\
 a_{i7} &= 0 \quad \forall i = 1, 5, 6, \dots, t+2 ; a_{47} = 2 ; a_{i7} \neq 0 \text{ pour } i = 2, 3 \\
 a_{i8} &= 0 \quad \forall i = 2, 5, 6, \dots, t+2 ; a_{48} = 2 ; a_{i8} \neq 0 \text{ pour } i = 1, 3 \\
 a_{i9} &= 0 \quad \forall i = 3, 5, 6, \dots, t+2 ; a_{49} = 2 ; a_{i9} \neq 0 \text{ pour } i = 1, 2 \\
 a_{i10} &= 0 \quad \forall i = 1, 4, 6, \dots, t+2 ; a_{5,10} = 1 ; a_{i,10} \neq 0 \text{ pour } i = 2, 3 \\
 a_{i11} &= 0 \quad \forall i = 2, 4, 6, \dots, t+2 ; a_{5,11} = 1 ; a_{i,11} \neq 0 \text{ pour } i = 1, 3 \\
 a_{i12} &= 0 \quad \forall i = 3, 4, 6, \dots, t+2 ; a_{5,12} = 1 ; a_{i,12} \neq 0 \text{ pour } i = 2, 3 \\
 a_{i13} &= 0 \quad \forall i = 1, 4, 6, \dots, t+2 ; a_{5,13} = 2 ; a_{i,13} \neq 0 \text{ pour } i = 2, 3 \\
 a_{i14} &= 0 \quad \forall i = 2, 4, 6, \dots, t+2 ; a_{5,14} = 2 ; a_{i,14} \neq 0 \text{ pour } i = 1, 3 \\
 a_{i15} &= 0 \quad \forall i = 3, 4, 6, \dots, t+2 ; a_{5,15} = 2 ; a_{i,15} = 0 \text{ pour } i = 1, 2
 \end{aligned}$$



Il en résulte que  $(a_{2j}, a_{3j}) \in \{1, 2\}^2$  pour  $j = 4, 7, 10, 13$   
 et si 2 de ces couples sont identiques cela entraîne l'égalité  
 de 2 t-uples dans les colonnes correspondantes. On a donc :

$$\{(a_{2j}, a_{3j}), \forall j = 4, 7, 10, 13\} = \{1, 2\}^2$$

D'autre part, nous avons, par exemple, :

$$(a_{22}, a_{32}) \in \{1, 2\}^2$$

et il existe donc  $j_1 \in \{4, 7, 10, 13\}$  tel que

$$(a_{22}, a_{32}) = (a_{2j_1}, a_{3j_1})$$

cela entraîne que les colonnes de rang 2 et  $j_1$  ont un t-uple en  
 commun (les éléments de la 2ème et de la 3ème ligne et t-2 éléments  
 égaux à 0 dans les t-1 dernières lignes).

Il n'existe donc pas de tableau orthogonal de t+2 lignes dans  
 ce cas.

3°)  $S > 3$  : soit  $a_{ij}$  l'élément de la ième ligne et de la jème  
 colonne. Nous supposons toujours que  $a_{i1} = 0, \forall i = 1, 2, \dots, t+2$  ;  
 et que  $a_{ij} = 0 \quad \forall i = 4, 5, 6, \dots, t+2$  pour  $j = 2, 3, \dots, S$  ;

De plus nous savons qu'il existe S colonnes telles que :

$$\begin{cases} a_{ij} = 0 & i \notin \{k, 1, 2, 3\} \\ a_{ij} = u & i = k \end{cases} \quad k > 3$$

et donc lorsque u varie dans  $\{1, 2, \dots, S-1\}$  et k varie dans  
 $\{4, 5, \dots, t+2\}$ , on obtient (t-1) (S-1) ensembles de S colonnes  
 distinctes des S premières colonnes.

Considérons un tel ensemble de S colonnes qui ont des (t-1)-uples  
 identiques. Pour un tel ensemble de colonnes chacune des 3  
 premières lignes du tableau doit être formée d'une permutation  
 des éléments 0, 1, 2, ..., S-1. Donc l'élément 0 doit intervenir



dans chacune des 3 premières lignes, mais ne doit pas être présent dans 2 de ces 3 premières lignes et dans la même colonne, sinon il apparaîtrait un t-uple formé de 0 uniquement ce qui est impossible car un tel t-uple apparaît déjà dans la 1ère colonne. Il y a donc  $(S-3)(t-1)(S-1)$  colonnes dans ces ensembles qui ne contiennent pas 0 dans l'une des 3 premières lignes. Soit  $e$  l'élément qui intervient le plus souvent dans la première ligne du tableau et dans ces  $(S-3)(t-1)(S-1)$  colonnes :  $e$  intervient dans ces colonnes et dans la 1ère ligne au moins  $(S-3)(t-1)$  fois.

$e$  intervient aussi dans la 1ère ligne d'une des  $S$  premières colonnes. Supposons que dans cette colonne l'élément de la 2ème ligne soit  $a$  et l'élément de la 3ème ligne soit  $b$ . Alors aucun élément de la 2ème ligne ne peut être  $a$  si la même colonne contient  $e$  dans sa 1ère ligne. Une remarque identique s'applique à  $b$ . (sinon on obtiendrait 2 colonnes possédant des t-uples identiques). Pour compléter les colonnes contenant  $e$  dans la 1ère ligne nous ne pouvons donc choisir qu'entre  $(S-2)^2$  doublets. Or les doublets choisis doivent être distincts et aucun de ces doublets ne peut coïncider avec un doublet occupant la même place dans l'ensemble des  $S$  premières colonnes. Or dans l'ensemble des  $S$  premières colonnes il y a  $(S-2)$  doublets distincts entre eux et distincts de  $(0,0)$  et de  $(a,b)$ .

Nous ne pouvons donc choisir que parmi  $(S-2)^2 - (S-2)$  doublets et nous devons donc avoir :

$$(S-2)^2 - (S-2) \geq (S-3)(t-1)$$

ou  $(3-S)(t-S+1) \geq 0$  ce qui est impossible puisque nous avons supposé  $S > 3$  et  $S \leq t$

Nous venons donc de montrer que  $f(1, S, t) \leq t+1$  lorsque  $S \leq t$ . Mais nous avons aussi montré (Théorème II.1.5.1) que quels que soient  $S$  et  $t$ , il existe toujours un tableau orthogonal  $(1, t+1, S, t)$ . Cela entraîne que  $f(1, S, t) = t+1$  si  $S \leq t$ .



Théorème IV.1.2 :

- Si  $t \leq S$  et si  $S$  est pair, alors  $f(1, S, t) \leq S + t - 1$
- Si  $3 \leq t \leq S$  et si  $S$  est impair, alors  $f(1, S, t) \leq S + t - 2$
- Si  $S = p^n$  ( $p =$  nombre premier impair)  $f(1, S, 3) = S + 1$
- Si  $S = 2^n$   $f(1, 2^n, 3) = S + 2$

Démonstration : 1°) Etant donné un tableau orthogonal  $(1, 3, S, 2)$ , on peut ajouter  $k$  lignes à ce tableau orthogonal pour en faire un tableau orthogonal  $(1, k+3, S, 2)$  si et seulement si il existe  $k$  familles de  $S$  transversales disjointes 2 à 2 du tableau orthogonal  $(1, 3, S, 2)$  telles que 2 transversales quelconques appartenant à 2 familles différentes aient au plus un élément en commun. Or, étant donné un triplet  $(x_1, y_1, z_1)$  colonne du tableau orthogonal  $(1, 3, S, 2)$ , une transversale du tableau  $(1, 3, S, 2)$  contenant ce triplet contiendra aussi dans sa 1ère ligne  $x_2$  (et il existe  $S$  colonnes de ce tableau ayant  $x_2$  dans sa 1ère ligne), mais ne contiendra pas  $y_1$  dans sa 2ème ligne (et il existe une colonne et une seule de ce tableau contenant  $x_2$  dans sa 1ère ligne et  $y_1$  dans sa 2ème ligne) et ne contiendra pas  $z_1$  dans sa 3ème ligne (et il existe une colonne et une seule de ce tableau contenant  $x_2$  dans sa 1ère ligne et  $z_1$  dans sa 3ème ligne). Il existe donc au plus  $S-2$  transversales ayant un élément  $(x_1, y_1, z_1)$  en commun et un seul. Il en résulte que  $k \leq S-2$  et que  $f(1, S, 2) \leq S+1$ . Or l'existence d'un tableau orthogonal  $T(1, r, S, t)$  entraîne celle d'un tableau orthogonal  $T'(1, r-1, S, t-1)$  (il suffit de considérer le sous-tableau formé par les  $S^{t-1}$  colonnes du tableau  $T$ , colonnes dont les éléments de la 1ère ligne sont tous identiques à un élément de l'ensemble sur lequel est construit  $T$ , et de supprimer ensuite la première ligne du tableau ainsi formé pour obtenir  $T'$  à partir de  $T$ ). Il en résulte que la non-existence de  $T'(1, r-1, S, t-1)$  entraîne la non existence de  $T(1, r, S, t)$  et en appliquant  $(t-2)$  fois ce résultat au tableau  $(1, S+1, S, 2)$



on obtient :  $f(1, S, t) \ll S+t-1$ .

2°) Supposons que pour  $t = 3$ , on puisse construire un tableau orthogonal  $(1, S+2, S, 3)$  sur  $E = \{0, 1, 2, \dots, S-1\}$ . Alors chaque élément est répété  $S^2$  fois dans chaque ligne et chaque doublet est répété  $S$  fois dans un couple de lignes. Considérons les éléments de la première colonne et soit  $a_1$  l'élément de la 1ère ligne dans cette 1ère colonne. Au moyen des autres éléments  $(a_2, a_3, \dots, a_{S+2})$  de cette 1ère colonne, on peut former  $S+1$  doublets  $(a_1, a_i)$  ( $i = 2, 3, \dots, S+2$ ).

Il en résulte que le nombre total de colonnes ayant  $a_1$  dans sa première ligne et  $a_i$  dans sa  $i$ ème ligne, quel que soit  $i = 2, 3, \dots, S+2$  est  $(S+1)(S-1)$  et l'on voit que ce nombre épuise toutes les répétitions de l'élément  $a_1$  dans la 1ère ligne du tableau.

Il en résulte que 2 colonnes du tableau ont ou bien un doublet en commun ou bien aucun élément en commun (dans une même ligne).

A partir des  $S+2$  éléments de la première colonne, nous pouvons former  $\frac{(S+2)(S+1)}{2}$  couples non ordonnés qui sont répétés  $(S-1)$  fois. Or  $\frac{(S+2)(S+1)(S-1)}{2} < S^3 - 1$  si  $S > 1$

Si bien qu'il existe des colonnes qui n'ont aucun élément en commun dans la même ligne.

Soit donc  $(\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{S+2}) = \alpha$

$(\beta_1, \beta_2, \dots, \beta_i, \dots, \beta_{S+2}) = \beta$

2 telles colonnes, c'est-à-dire que  $\alpha_i \neq \beta_i, \forall i = 1, 2, \dots, S+2$

Il existe  $(S-1)$  colonnes  $\gamma^j$  ( $j = 1, 2, \dots, S-1$ ) distinctes de  $\beta$  mais telles que  $\gamma_1^j = \beta_1, \gamma_2^j = \beta_2$  (l'élément de la  $i$ ème ligne de la colonne  $\gamma^j$  est  $\gamma_i^j$ ).

Le tableau orthogonal étant de force 3,

$$\{\beta_i\} \cup \{\gamma_i^j, \forall j = 1, 2, \dots, S-1\} = E \text{ pour } i = 3, 4, \dots, S+2$$



Il existe donc  $j_i \in \{1, 2, \dots, S-1\}$  tel que  $\alpha_i = \gamma_i^{j_i}$  (pour  $i = 3, 4, \dots, S+2$ ) et comme les colonnes  $\alpha$  et  $\gamma^{j_i}$  ont déjà un élément en commun dans la ligne  $i$  il est nécessaire qu'elles en aient un autre en commun dans une autre ligne. Les  $S$  éléments  $a_3, a_4, \dots, a_{S+2}$  doivent donc se partager en couples, chaque couple se retrouvant à la même place dans une des colonnes  $\gamma^j$ . Or cela est impossible si  $S$  est impair. Donc si  $S$  est impair  $f(1, S, 3) \leq S + 1$ . Par le même raisonnement que celui que nous avons fait à la fin du 1°) de cette démonstration, on montre que cela entraîne que  $f(1, S, t) \leq S+t-2$  si  $S$  est impair et  $S \geq t \geq 3$ . Dans le cas  $t = 3$ , le théorème II.5.1 et la remarque II.5.1 montrent qu'il existe des tableaux orthogonaux  $(1, S+1, S, 3)$  si  $S = p^n$  et des tableaux orthogonaux  $(1, S+2, S, 3)$  dans le cas particulier  $S = 2^n$ .

#### IV.2 : Tableaux orthogonaux de force 2 et de force 3 : [III]

##### Théorème IV.2.1 :

- 1)  $f(\lambda, S, 2) \leq$  partie entière de  $\left(\frac{\lambda S^2 - 1}{S-1}\right)$
- 2) si  $(\lambda - 1)$  n'est pas divisible par  $(S-1) : \lambda - 1 = a(S-1) + b$ ,  
 $0 < b < S-1$  alors  $f(\lambda, S, 2) \leq$  partie entière de  
 $\left(\frac{\lambda S^2 - 1}{S-1}\right) -$  partie entière de  $(\theta) - 1$   
 avec  $\theta = \frac{\sqrt{1 + 4 S(S-1-b)} - (2S - 2b - 1)}{2}$

Démonstration : Nous dirons que 2 colonnes

$$\alpha = (a_1, a_2, \dots, a_1, \dots, a_r)$$

$$\beta = (b_1, b_2, \dots, b_1, \dots, b_r)$$

d'un tableau orthogonal  $(\lambda, r, S, t)$  ont  $k$  coïncidences si



$$a_{j_f} = b_{j_f} \quad \text{pour } j_f \in \{j_1, j_2, \dots, j_k\} \subset \{1, 2, \dots, r\}$$

$$a_{j_f} \neq b_{j_f} \quad \text{pour } j_f \notin \{j_1, j_2, \dots, j_k\}$$

Si on appelle  $n_i$  le nombre de colonnes ayant  $i$  coïncidences avec la 1ère colonne d'un tableau orthogonal  $(\lambda, r, S, t)$ , nous avons la relation :

$$\sum_{i=0}^r n_i = \lambda S^t - 1$$

Si on considère le tableau obtenu à partir du précédent en prenant  $h < t$  lignes du précédent, on retrouve dans le nouveau tableau la 1ère colonne  $\lambda S^{t-h}$  fois.

Donc dans le tableau orthogonal  $(\lambda, r, S, t)$ , le nombre total de  $h$ -uples apparaissant dans les colonnes différentes de la première, mais coïncidant avec le  $h$ -uplet correspondant de la première colonne est :  $C_r^h (\lambda S^{t-h} - 1)$ .

Mais étant donnée une colonne ayant  $i$  coïncidences avec la première, on en déduit  $C_i^h n_i$   $h$ -uples coïncidant avec le  $h$ -uplet correspondant de la première. On a donc finalement

$$\sum_{i=0}^r n_i C_i^h = C_r^h (\lambda S^{t-h} - 1)$$

$$(C_i^h = 0 \text{ si } i < h)$$

Dans le cas  $t = 2$ , nous avons successivement en faisant  $h = 0$ ,  $h = 1$ , et  $h = 2$  :

$$\sum_{i=0}^r n_i = \lambda S^2 - 1 \quad (1)$$

$$\sum_{i=1}^r i \cdot n_i = r(\lambda S - 1) \quad (2)$$

$$\sum_{i=2}^r i(i-1) n_i = r(r-1)(\lambda - 1) \quad (3)$$



Considérons la fonction

$$f(x) = \sum_{i=0}^r (i-x)(i-1-x) n_i$$

définie pour  $x$  entier et positif.

On a  $f(x) \geq 0$

$$\text{Soit } \sum_{i=0}^r i(i-1) n_i - 2x \sum_{i=0}^r i n_i + x(x+1) \sum_{i=0}^r n_i \geq 0$$

et compte tenu des relations (1), (2), (3) :

$$\lambda [r(r-1) - 2r Sx + x(x+1)S^2] - [r(r-1) - 2rx + x(x+1)] \geq 0$$

$$\text{Or } r(r-1) - 2rSx + x(x+1)S^2 = (Sx - r)(Sx - (r-1)) + (S-1) Sx > 0$$

dès que  $S \geq 2$  ( $x \geq 0$ ) donc :

$$\lambda \geq \frac{r(r-1) - 2rx + x(x+1)}{r(r-1) - 2r S x + x(x+1) S^2}$$

Posons  $\alpha = r - 1 - Sx$ , on obtient

$$(4) \frac{\lambda S^2 - 1}{S-1} \geq r \left[ 1 + \frac{\alpha(S-\alpha)}{D} \right] \text{ avec } D = (S-1)(r-\alpha+1) + \alpha(\alpha+1)$$

Soit  $\lambda - 1 = a(S-1) + b$ ,  $a \geq 0$ ,  $0 \leq b < S-1$

$$\text{Alors } \frac{\lambda S^2 - 1}{S-1} = \lambda S + a + \frac{b}{S-1} + \lambda \quad (5)$$

Supposons qu'il existe un tableau orthogonal tel que

$$r = \lambda S + \lambda + a + 1$$

$$\text{alors } r - 1 = S(\lambda + a) + b + 1$$

Prenons  $x = \lambda + a$ , alors

$$\alpha = b + 1 \text{ et } D = S(S-1)(\lambda + a) + \alpha(\alpha + 1) > 0$$

si bien que  $\frac{\alpha(S-\alpha)}{D} > 0$  et on obtient, compte tenu des relations (4)



et (5) :  $\frac{b}{S-1} > 1$  ce qui est en contradiction avec l'inégalité  
 $0 \leq b < S-1$

Il en résulte que  $r < \lambda S + \lambda + a + 1$

et donc que  $r \leq$  partie entière de  $\left(\frac{\lambda S^2 - 1}{S-1}\right)$

Si  $\lambda - 1$  n'est pas divisible par  $S-1$ , c'est-à-dire si  $b \neq 0$

Prenons alors  $r = \lambda S + \lambda + a - n$ ,  $0 \leq n < b$

on a alors  $r - 1 = S(\lambda + a) + b - n$

On prend comme ci-dessus  $x = \lambda + a$  et alors  $0 < \alpha = b - n < S - 1$   
 $(\alpha + 1)(S - 1 - \alpha) > 0$

et  $D = r(S-1) - (\alpha + 1)(S - 1 - \alpha) > r(S - 1)$

et compte tenu de (4) :

$$\frac{\lambda S^2 - 1}{S - 1} > r + \frac{\alpha(S - \alpha)}{S - 1}$$

Soit :  $\frac{b}{S-1} > -n + \frac{(b-n)(S-b+n)}{S-1}$

et donc  $(b-n)(b+1-n) - S(b-2n) > 0$

Donc si  $n$  est un entier pour lequel la dernière relation n'est pas satisfaite, alors  $r = \lambda S + \lambda + a - n$  et toutes les valeurs supérieures seront impossibles.

Or  $(b-n)(b+1-n) \geq 0$ , si bien que pour  $n > \frac{b}{2}$

cette relation ne sera pas contredite. L'équation du 2ème degré en  $n$  obtenue en remplaçant l'inégalité précédente par l'égalité correspondante a une racine  $> 0$  et une racine  $< 0$  : en effet le produit des racines est  $< 0$  :  $-b(S-1-b) < 0$



La racine positive s'écrit

$$\theta = \frac{\sqrt{1 + 4 S(S - 1 - b)} - (2S - 2b - 1)}{2}$$

La plus grande valeur de  $n$  qui contredit la dernière inégalité est donc la partie entière de  $\theta$

et nous avons  $r < \text{partie entière de } \left( \frac{\lambda S^2 - 1}{S - 1} \right) - \text{partie entière de } \theta$   
et donc  $r \leq \text{partie entière de } \left( \frac{\lambda S^2 - 1}{S - 1} \right) - \text{partie entière de } \theta - 1$

Théorème IV.2.2. :

1)  $f(\lambda, S, 3) \leq \text{partie entière de } \left( \frac{\lambda S^2 - 1}{S - 1} \right) + 1$

2) si  $(\lambda - 1)$  n'est pas divisible par  $(S - 1)$  :  $\lambda - 1 = a(S - 1) + b$ ,  
 $0 < b < S - 1$

alors  $f(\lambda, S, 3) \leq \text{partie entière de } \left( \frac{\lambda S^2 - 1}{S - 1} \right) - \text{partie entière de } \theta$   
avec 
$$\theta = \frac{\sqrt{1 + 4 S(S - 1 - b)} - (2S - 2b - 1)}{2}$$

3) si  $(\lambda - 1)$  est divisible par  $(S - 1)$  :  $\lambda - 1 = a(S - 1)$   
et si  $(S - 1)^2 (S - 2)$  n'est pas divisible par  $a S + 2$ ,  
alors  $f(\lambda, S, 3) \leq \frac{\lambda S^2 - 1}{S - 1} - 1$

Démonstration : 1) et 2) : reprenons les notations employées dans la démonstration du théorème précédent, on a les relations

$$\sum_{i=0}^r n_i = \lambda S^3 - 1$$

$$\sum_{i=0}^r i n_i = r(\lambda S^2 - 1)$$

$$\sum_{i=0}^r i(i-1) n_i = r(r-1)(\lambda S - 1)$$



$$\sum_{i=0}^r i(i-1)(i-2) n_i = r(r-1)(r-2)(\lambda - 1)$$

On considère ensuite la fonction :

$$f(x) = \sum_{i=0}^r i(i-1-x)(i-2-x) n_i \geq 0 \text{ pour } x \text{ entier positif}$$

On obtient l'inégalité :

$$\lambda \geq \frac{(r-1)(r-2) - 2x(r-1) + x(x+1)}{(r-1)(r-2) - 2x(r-1) S + x(x+1) S^2}$$

inégalité analogue à celle obtenue pour  $t = 2$  et qui se transforme en cette dernière lorsque l'on y change  $r-1$  en  $r$

On en déduit donc comme dans la démonstration du théorème précédent les 2 premières majorations des contraintes énoncées dans le théorème IV.2.2

3) Nous avons dans ce cas

$$\frac{\lambda S^2 - 1}{S - 1} = \lambda S + \lambda + a = a S^2 + S + 1$$

Supposons que  $r = a S^2 + S + 1$

Choisissons  $x = aS$ , nous avons alors

$$f(aS) = \sum_{i=0}^r i(i-1-aS)(i-2-aS) n_i = 0$$

Comme  $n_i \geq 0$ , il s'en suit que  $n_i = 0$ ,  $\forall i$  sauf pour

$$i = 0, \quad i = aS + 1, \quad i = aS + 2$$

On a donc les 2 égalités

$$\begin{cases} (aS + 1) n_{aS+1} + (aS + 2) n_{aS+2} = r(aS^3 - aS^2 + S^2 - 1) \\ aS(aS+1) n_{aS+1} + (aS+1)(aS+2) n_{aS+2} = r(r-1)(aS^2 - aS + S - 1) \end{cases}$$

ou



$$\begin{cases} (aS+1) n_{aS+1} + (aS+2) n_{aS+2} = r(aS^3 - aS^2 + S^2 - 1) \\ aS n_{aS+1} + (aS+2) n_{aS+2} = rS(aS^2 - aS + S - 1) \end{cases}$$

système dont la solution est :

$$n_{aS+1} = r(S-1)$$

$$n_{aS+2} = \frac{rS(aS^2 - 2aS + a + S - 1)}{aS + 2}$$

$$\text{ou } n_{aS+2} = r(S-1)^2 - S(S-1)(S-2) + \frac{(S-1)^2 (S-1)}{aS+2}$$

Comme  $n_{aS+2}$  doit être entier, nous arrivons à une contradiction si  $(S-1)^2 (S-2)$  n'est pas divisible par  $aS+2$ .



BIBLIOGRAPHIE

- [I] BOSE (R.C.) Mathematical theory of the symmetrical factorial designs  
Sankhya (1947), Vol. 8, n° 2 p.107-166
- [II] BOSE (R.C.) On some corrections between the design of experiments and information theory  
Bull. int. Stat. inst. (1960)  
32e session (Tokyo)
- [III] BOSE (R.C.) Orthogonal arrays of strength two and three  
BUSH (K.A.) Ann. Math. Stat. (1952), vol. 23,  
p. 508-524
- [IV] BOSE (R.C.) On a class of error correcting binary  
RAY CHAUDURI (D.K.) groups codes. Information and control  
(1960), Vol. 3, n° 1, p. 68-79
- [V] BUSH (K.A.) Orthogonal arrays of index unity  
Ann. Math. Stat. (1952), Vol. 23,  
p. 426-434
- [VI] CARMICHAEL (R.D.) Introduction to the theory of groups  
of finite order (Dover Publications)
- [VII] HALL (M.) The theory of groups (Mac Millan  
Compagny)
- [VIII] JORDAN (C.) Traité des substitutions et des équations  
algébriques (Gauthier-Villars)
- [IX] MASUYAMA (M.) On difference sets for constructing  
orthogonal arrays of index two and  
of strength two  
Report. Stat. appl. Res. (1959), vol.5,  
n° 1, p. 27-34



- [X] MAURIN (F.) Sur une généralisation de la méthode des différences pour la construction de tableaux orthogonaux.  
C.R. Acad. Sc. Paris (1964), p.4490-4491
- [XI] MAURIN (F.) Sur certains groupes de substitutions entraînant l'existence de tableaux orthogonaux.  
C.R. Acad. Sc. Paris (1965), p. 52-55
- [XII] MAURIN (F.) Automorphismes propres de groupes et groupes abéliens finis sous-transitifs d'ordre  $t$  et d'indice unité. Application à la construction des tableaux orthogonaux.  
C.R. Acad. Sc. Paris (1966), p.1194-1197
- [XIII] MAURIN (F.) Automorphismes propres de groupes abéliens finis et orthomorphismes de groupes finis. Application à la construction de tableaux orthogonaux.  
C.R. Acad. Sc. Paris (1967), p.702-704
- [XIV] MAURIN (F.) Sur une modification d'une méthode de Yamamoto pour la construction de tableaux orthogonaux de force 2. Généralisation au cas de tableaux orthogonaux de force quelconque.  
C.R. Acad. Sc. Paris (1968), p. 1262-1265
- [XV] MAURIN (F.) Sur une généralisation d'une méthode de Sade pour la construction de tableaux orthogonaux  
C.R. Acad. Sc. Paris (1969), p. 109-112



- [XVI] PLACKETT (R.L.) BURMAN (J.P.) The design of optimum multifactorial experiments. Biometrika (1943-46), Vol 33, p. 305
- [XVII] RAO (C.R.) On hypercubes of strength d and a system of confounding in factorial experiments Bull. Cal. Math. Soci. (1946), vol. 38, p. 143-164
- [XVIII] RAO (C.R.) Factorial experiments derivable from combinatorial arrangements of arrays J.Roy. Stat. Soc. (suppl). (1947) p. 128-139
- [XIX] SADE Produit direct singulier de quasi-groupes orthogonaux et anti-abéliens An. Soc. Scien. Bruxelles (1960), Tome 74, p. 91-99
- [XX] SEIDEN On the maximum number of constraints of an orthogonal array Ann. Math. Stat. (vol.26) p. 132-135
- [XXI] SEIDEN A theorem in finite projective geometry and an application to statistics Proc. Amer. Math. Soc. (1950) vol. 1, p. 282-286
- [XXII] YAMAMOTO Generation principles of Latin Squares I.S.I. (1960) 32e session (Tokyo)



## DEUXIÈME THÈSE

---

Propositions données par la Faculté

"Martingales et théorèmes de convergence."

Vu et approuvé

Paris, le 13 Avril ..... 1970

Le Doyen de la Faculté des Sciences  
de Paris

Marc. ZAMANSKY

Vu  
et permis d'imprimer

Le Recteur de l'Académie de Paris

Robert MALLET





